PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-056449
(43)Date of publication of application : 24.02.1998

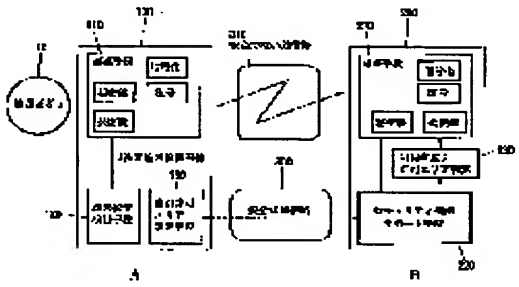
(51)Int.Cl. H04L 9/32
G01S 5/02
G06F 15/00
G06F 17/60
G06F 19/00
G09C 1/00
H04Q 7/36
H04Q 7/34
H04Q 7/38

(21)Application number : 08-211299
(22)Date of filing : 09.08.1996

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : YOSHIDA TETSUO

(54) SECURITY STRENGTHENING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To strengthen a security function even in the case of utilizing a non- safety communication path by excluding the danger of 'successful impersonating' due to an illegal user by completing user identification with the terminal position information of a terminal position detecting means and an area setting/ discriminating means or the like.
SOLUTION: A terminal (A) 100 of a person to be verified is provided with a terminal position detecting means 120 for always detecting its present position by detecting a sensor terminal itself for detecting the direction, attitude and three-dimensional movement of the terminal together with a verifying means 110 and a transaction permission area setting means 130 for making the terminal position and a transaction permission area correspondent on a stereoscopic map. Besides, a server (B) 200 of a verifying person is provided with a security function support means 220 for preserving the password of every user and the data of the transaction permission area and referring to them at the time of verification together with a verifying means 210 and an area discriminating means 230 for discriminating the permission of transaction based on these data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－56449

(43)公開日　平成10年(1998)２月24日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７３Ｚ
Ｇ０１Ｓ	5/02			Ｇ０１Ｓ	5/02	Ｚ
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｂ
	17/60		7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｇ
	19/00			Ｇ０６Ｆ	15/21	３４０Ｂ

審査請求　未請求　請求項の数13　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－211299

(22)出願日　平成８年(1996)８月９日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　吉田　哲雄
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

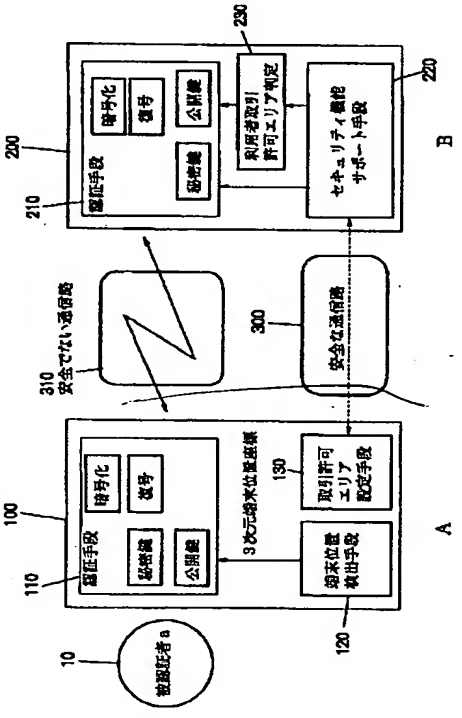
(74)代理人　弁理士　前田　実

(54)【発明の名称】　セキュリティ強化システム

(57)【要約】

【課題】　不正な利用者による「なり済まし」の危険性を排除して、安全でない通信路を利用する場合においてもセキュリティ機能を強化するセキュリティ強化システムを提供する。

【解決手段】　セキュリティ強化システムは、通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法において、端末「Ａ」１００が、端末位置を検出する「端末位置検出手段」１２０と、取引許可エリアを設定する「許可エリア設定手段」１３０とを備え、サーバ「Ｂ」２００が、「許可エリア設定手段」１３０により設定された各ユーザの登録エリアを保存する「セキュリティ機能サポート手段」２２０と、「端末位置検出手段」１２０により検出された端末位置が登録エリアにあることを判定する「利用者取引許可エリア判定手段」２３０とを備え、端末位置情報により、利用者認証を補完する。



1

【特許請求の範囲】

【請求項１】　通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法のセキュリティ強化システムであって、

被認証者の装置は、端末位置を検出する端末位置検出手段と、

取引許可エリアを設定する許可エリア設定手段とを備え、

認証者の装置は、上記許可エリア設定手段により設定された各ユーザの登録エリアを保存する登録エリア保存手段と、

上記端末位置検出手段により検出された端末位置が上記登録エリアにあることを判定するエリア判定手段とを備え、

上記端末位置情報により、利用者認証を補完することを特徴とするセキュリティ強化システム。

【請求項２】　上記通信回線を介して授受されるディジタル情報は、

上記端末位置情報を暗号化して上記認証者の装置に送信することを特徴とする請求項１記載のセキュリティ強化システム。

【請求項３】　上記端末位置検出手段は、

端末本体の変位を検出する運動センサを備えたことを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項４】　上記端末位置検出手段は、

移動体通信システムにより位置情報を獲得する位置情報獲得手段を備えたことを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項５】　上記端末位置検出手段は、

移動体通信システムにより位置情報を獲得する位置情報獲得手段と、

端末本体の変位を検出する運動センサとを備え、

上記位置情報獲得手段による位置情報及び上記運動センサによる変位データに基づいて端末位置を検出することを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項６】　上記端末位置検出手段は、

外部からの信号により位置情報を検出する位置検出手段を備えたことを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項７】　上記端末位置検出手段により得られた端末位置情報を、前記位置検出手段により校正する校正手段を備えたことを特徴とする請求項１、２又は６の何れかに記載のセキュリティ強化システム。

【請求項８】　上記端末位置検出手段は、

外部からの信号により位置情報を検出する位置検出手段と、

運動センサによる変位検出手段と、

外部からの信号の受信状況を判定する判定手段とを備え、

2

上記判定手段の判定に基づいて上記変位検出手段の変位データにより上記端末位置情報を補正することを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項９】　上記外部からの信号は、ＧＰＳの衛星航法電波信号であることを特徴とする請求項６、７又は８の何れかに記載のセキュリティ強化システム。

【請求項１０】　上記請求項１又は２の何れかに記載のセキュリティ強化システムにおいて、

上記登録エリア保存手段へのエリア登録の通信路を限定することを特徴とするセキュリティ強化システム。

【請求項１１】　上記認証者の装置は、

被認証者の認証要求の再試行許可回数を登録する手段を備え、

認証要求時に授受するディジタル情報に付加された位置情報と予め登録済のエリア情報によるエリア判定手段の判定結果が不正となる回数が、上記再試行許可回数を超えた場合に取引禁止処理を行うことを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項１２】　上記被認証者の端末が車載用の端末であって、端末位置情報を車載用のナビゲーションシステムから得ることを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【請求項１３】　上記被認証者の装置又は上記認証者の装置は、

上記端末位置検出手段の検出位置を校正する検出位置校正手段と、

上記検出端末位置校正手段の設定、上記許可エリア設定手段の設定、あるいは上記許可エリア設定手段の表示を許可する端末の場所、のうち少なくとも何れか１つ以上を限定する限定手段とを備えたことを特徴とする請求項１又は２の何れかに記載のセキュリティ強化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークセキュリティのセキュリティ強化システムに係り、特に、移動端末における利用者認証におけるセキュリティ強化システムに関する。

【０００２】

【従来の技術】近年、ネットワークを介しての電子商取り引きが実現しつつあり、固定の閉じた公衆回線を用いる場合は、ユーザＩＤとパスワードあるいは口座番号と暗証番号により取引の安全を確保しているが、特にインターネットのようなオープンなネットワークを用いる場合においては、情報セキュリティや利用者認証が重要な課題となってきている。

【０００３】更に移動体端末のようにどこからでもネットワークを介しての商取り引きが可能となると、従来のように端末設置場所に不法な利用者が侵入できなければ

安全であるということはできず、安全なオンライン商取り引きを実現するためには利用者認証が必須技術となる。

【０００４】認証方法の代表的な例として、ＲＳＡ暗号系を利用したものがある。例えば、「ネットワークにおける情報セキュリティ技術とサービス」テレビジョン学会誌Ｖｏｌ．４９，Ｎｏ．１２，ｐｐ．１５６７～１５７１（１９９５）に記載されたものがある。

【０００５】上記文献には、ＲＳＡ暗号方式の概要とＲＳＡ暗号方式を用いた情報保護システムについて記載されている。

【０００６】暗号アルゴリズムは大きく分けて、共通鍵暗号と公開鍵暗号の２方式があり、ＲＳＡは公開鍵暗号の代表例である。共通鍵暗号が、暗号化鍵と復号鍵が同じ鍵で、送り手、受け手がお互いに秘密に保持して暗号化、復号を高速に実現するのに対して、ＲＳＡに代表される公開鍵暗号は、暗号化鍵と復号鍵が異なり、公開された受け手の暗号化鍵により誰でも通信文を暗号化でき、正規の受け手のみが持つ秘密鍵により復号する。暗号化と復号の順序を逆にすると、秘密鍵を保有する人のみが秘密変換（ディジタル署名）でき、その人の公開鍵を知っている誰もが公開変換（署名の検証）できる性質がある。

【０００７】この性質を利用して、通信相手の認証及び通信事実の証明が安全・確実に実現されるのである。

【０００８】このＲＳＡ公開暗号方式のＲＳＡは、ＭＩＴにおける開発者Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｌｅｍａｎの３名の頭文字より命名されている。ＲＳＡ暗号方式のアルゴリズムを図１１に示す。

【０００９】この方式においては２種類の暗号鍵を作る。一方は秘密鍵と呼ばれ持ち主のみが保管する。もう一方は公開鍵と呼ばれ、相手に渡す。

【００１０】図１１において、ｄは秘密鍵を表し、（ｅ，ｎ）は公開鍵を表す。秘密鍵で暗号化して得られる暗号文は対応する公開鍵でしか復号できず、逆に公開鍵で暗号化した暗号文は対応する秘密鍵でしか復号できない。暗号化及び復号の関数において、「ａ　ｍｏｄ　ｎ」はａをｎで割った時の余りを表す。

【００１１】利用者Ａが利用者Ｂにメッセージを送る場合を例にとり具体的に説明する。

【００１２】ＡとＢはお互いに相手の公開鍵を持っているとする。第１の方法は、ＡがＢの公開鍵で暗号化する方法、第２の方法はＡが自分の秘密鍵で暗号化する方法である。

【００１３】第１の方法では、Ａの送ったメッセージはＢの秘密鍵でしか解読できないので情報の秘密性を第三者に対して守ることができる。第２の方法では、ＡがＢに送ったメッセージは、Ａの秘密鍵でしか作れないので、送り主がＡであることが保証され、その内容も改ざんされていないと考えられる。

【００１４】第２の方法によってＡが本人である認証ができるので、ディジタル署名として利用できるが、Ａの公開鍵を持っていれば解読できるので第１の方法と併用することにより、同時にデータの保護も実現できるのである。

【００１５】この方式の安全性は、ｎが大きい時の大きな素因数分解の難しさに依存しており、鍵の総当たりによる方法以外の解読法が見つかっていないため、最も信頼される公開鍵暗号方式の一つとされている。

【００１６】

【発明が解決しようとする課題】しかしながら、公開鍵から秘密鍵を作成するアルゴリズムを発見したり、第三者が秘密鍵を入手する危険性が全くないわけではなく、鍵が短い程秘密鍵を解読しやすく、安全でない通信路を介しての利用においては特に問題となる。また、理論的に危険性を小さくしても、秘密鍵を含む利用者カードや端末が不正利用者の手に渡った場合には「他人になり済まし」による不正利用の危険性を防ぐことはできない。

【００１７】特に、秘密鍵が利用者カードや携帯端末のように可搬性を有する場合には、ネットワークを介してその情報が不正に盗まれる危険性を排除しても、利用者カードや携帯端末が邪悪な第三者の手に渡る危険性は残る。

【００１８】本発明は、かかる不正な利用者による「なり済まし」の危険性を排除して、安全でない通信路を利用する場合においてもセキュリティ機能を強化するセキュリティ強化システムを提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明に係るセキュリティ強化システムは、通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法のセキュリティ強化システムであって、被認証者の装置は、端末位置を検出する端末位置検出手段と、取引許可エリアを設定する許可エリア設定手段とを備え、認証者の装置は、許可エリア設定手段により設定された各ユーザの登録エリアを保存する登録エリア保存手段と、端末位置検出手段により検出された端末位置が登録エリアにあることを判定するエリア判定手段とを備え、端末位置情報により、利用者認証を補完する。

【００２０】また、通信回線を介して授受されるディジタル情報は、端末位置情報を暗号化して認証者の装置に送信するようにしてもよく、端末位置検出手段は、端末本体の変位を検出する運動センサを備えたものであってもよい。

【００２１】また、端末位置検出手段は、移動体通信システムにより位置情報を獲得する位置情報獲得手段を備えたものであってもよく、端末位置検出手段は、移動体通信システムにより位置情報を獲得する位置情報獲得手段と、端末本体の変位を検出する運動センサとを備え、位置情報獲得手段による位置情報及び運動センサによる

変位データに基づいて端末位置を検出するものであってもよい。

【００２２】また、端末位置検出手段は、外部からの信号により位置情報を検出する位置検出手段を備えたものであってもよく、端末位置検出手段により得られた端末位置情報を、前記位置検出手段により校正する校正手段を備えたものであってもよい。

【００２３】また、端末位置検出手段は、外部からの信号により位置情報を検出する位置検出手段と、運動センサによる変位検出手段と、外部からの信号の受信状況を判定する判定手段とを備え、判定手段の判定に基づいて変位検出手段の変位データにより端末位置情報を補正するようにしてもよく、外部からの信号は、ＧＰＳの衛星航法電波信号であってもよい。

【００２４】また、上記セキュリティ強化システムは、登録エリア保存手段へのエリア登録の通信路を限定するようにしてもよい。

【００２５】また、認証者の装置は、被認証者の認証要求の再試行許可回数を登録する手段を備え、認証要求時に授受するディジタル情報に付加された位置情報と予め登録済のエリア情報によるエリア判定手段の判定結果が不正となる回数が、再試行許可回数を超えた場合に取引禁止処理を行うようにしてもよい。

【００２６】また、被認証者の端末が車載用の端末であって、端末位置情報を車載用のナビゲーションシステムから得るものであってもよい。

【００２７】さらに、被認証者の装置又は認証者の装置は、端末位置検出手段の検出位置を校正する検出位置校正手段と、検出端末位置校正手段の設定、許可エリア設定手段の設定、あるいは許可エリア設定手段の表示を許可する端末の場所、のうち少なくとも何れか１つ以上を限定する限定手段とを備えたものであってもよい。

【００２８】

【発明の実施の形態】本発明に係るセキュリティ強化システムは、インターネット等のオープンなネットワークを用いる電子商取引の利用者の認証機能強化に利用可能なセキュリティ強化システムに適用することができる。

【００２９】図１は本発明の第１の実施形態に係るセキュリティ強化システムの構成を示すブロック図である。

【００３０】図１において、「Ａ」は可搬の被認証者の端末１００（被認証者の装置）、「Ｂ」は「Ａ」の利用者及びその他の利用者を認証し、商取引サービスを提供するサーバ２００（認証者の装置）である。

【００３１】まず、端末「Ａ」１００及びサーバ「Ｂ」２００は、上述した従来技術と同様のＲＳＡ暗号系「認証手段」１１０及び２１０を備える。

【００３２】更に、端末「Ａ」１００は、端末の方向、姿勢及び３次元的な運動を検出するセンサ端末自身の位置を検出して、端末の現在地を常に検出する「端末位置検出手段」１２０と、立体的な地図上に端末位置及び取引許可エリアを対応付けることを可能にするグラフィック・ユーザ・インタフェース機能を含む「取引許可エリア設定手段」１３０とを備える。

【００３３】ここでの立体的な地図とは、平面的な配置に加えて、建物の上下方向のどのフロアであるかが区別できる程度の地図をいう。

【００３４】また、サーバ「Ｂ」２００は各ユーザのパスワード及び取引許可エリアのデータを安全に保管し、認証時に参照する「セキュリティ機能サポート手段」２２０（登録エリア保存手段）と、上記データに基づいて取引許可の判定を行う「利用者取引許可エリア判定手段」２３０（エリア判定手段）とを備える。

【００３５】端末「Ａ」１００とサーバ「Ｂ」２００との間は、ネットワークを介して通信を行うが、「特別な場所」においては、安全性の保証された「安全な通信路」３００により通信することが可能で、その他の場所では、利便性から「安全でない通信路」３１０を利用するものとする。

【００３６】ここでいう「安全な通信路」３００とは、一般的に盗聴不可能で契約外の第三者が許可なく同一アドレスあるいは電話番号を用いて通信できない回線、あるいはオープンな回線であっても、暗号技術等のセキュリティ技術により、前記と同等の安全性が保証された回線をいう。これに対して、「安全でない通信路」３１０とは、専門知識と設備を有する第三者が通信データを盗むことが技術的に可能とされる回線をいう。

【００３７】図１においては、利用者である「被認証者ａ」１０一人のみが示されているが、一般的な応用においては複数の同様のユーザ及び複数の端末が存在し、「被認証者ａ」はその内の一人を示すことになる。また、物理的に同一の端末を複数の利用者が利用し、かつ利用者毎に区別して認証することなども可能であり、複数の利用者の構成によっては、別の暗号鍵を用いるようにすることも可能である。

【００３８】この場合、図１では暗号鍵が端末内に備えられているように構成されているが、端末と分離可能な「ＩＣカード」、「利用者カード」などに実装することも可能である。

【００３９】次に、上述のように構成されたセキュリティ強化システムの動作を説明する。

【００４０】図２は図１の構成におけるセキュリティ強化システムの動作を説明するためのフローチャートであり、以下ステップ順に説明する。

【００４１】＜ステップ１＞図１において、端末「Ａ」１００の利用者である「被認証者ａ」１０は、端末「Ａ」１００の「端末位置検出手段」１２０の初期設定を行う。この初期設定は、端末の現在地とその方向を、システムが有する地図上の「特別な場所」の座標と方向に校正することであり、「被認証者ａ」１０が「特別な場所」から「安全な通進路」３００を用いてサーバ

「Ｂ」２００による認証を受けてのみ「被認証者ａ」１０による端末「Ａ」１００の「端末位置検出手段」１２０の初期設定を許可することにより、第三者が不正取引を目的に不正な設定をするのを防止する。このような「特別な場所」においては、サーバ「Ｂ」２００との間に「安全な通信路」３００が確保されているものとする。

【００４２】＜ステップ２＞端末「Ａ」１００の利用者である「被認証者ａ」１０は、端末「Ａ」１００を用いての商取引を許可するエリアを端末「Ａ」１００の「取引許可エリア設定手段」１３０のグラフィック・ユーザ・インタフェースを用いてサーバ「Ｂ」２００の「セキュリティ機能サポート手段」２２０に登録する。一般的に、この登録作業は「特別な場所」において行う。この「特別な場所」においても、サーバ「Ｂ」２００との間に「安全な通信路」３００が確保されているものとする。

【００４３】＜ステップ３＞以下、端末「Ａ」１００を上記＜ステップ２＞で予め設定しておいた「特別な場所」以外に持ち運んだ場合を例にとる。「安全な通信路」３００ではないため「安全でない通信路」３１０により取引を行うために、まずサーバ「Ｂ」２００と通信を開始する。

【００４４】＜ステップ４＞被認証者「ａ」１０はサーバ「Ｂ」２００の公開鍵を用いて、自分のユーザＩＤコードを送信する。

【００４５】＜ステップ５＞サーバ「Ｂ」２００は、サーバ「Ｂ」２００の秘密鍵を用いて、送られてきたユーザＩＤコードを特定する。この時点では、ユーザＩＤコードを送った利用者が本人であるかどうかは確認できないが、サーバ「Ｂ」２００の秘密鍵はサーバ以外には知られていないため、第三者にユーザＩＤコードが盗まれることはない。

【００４６】サーバ「Ｂ」２００は、特定されたユーザに対して、パスワードと取引の種類等を質問する。

【００４７】＜ステップ６＞被認証者「ａ」１０は、自分のパスワードと取引データを秘密鍵（この場合、端末「Ａ」１００の秘密鍵）で暗号化して送信する。この時、端末「Ａ」１００の位置情報も自動的に付加され、同時に暗号化されて送信する。

【００４８】秘密鍵（端末「Ａ」１００の秘密鍵）での暗号化に加えて、更にサーバ「Ｂ」２００の公開鍵で暗号化することにより被認証者「ａ」１０の公開鍵を入手した第三者によりパスワード、取引データ、位置情報が盗まれる危険性を排除することができる。

【００４９】＜ステップ７＞サーバ「Ｂ」２００は上記＜ステップ５＞で特定したユーザの公開鍵（すなわち、端末「Ａ」１００の公開鍵）で復号することで被認証者「ａ」１０が本人であると認証し、取引データも改ざんされていないことを確信するが、更に「端末位置検出手段」１２０によって自動的に付加された位置情報が、予め登録されていた取引許可エリアにあることをチェックして正当な取引者であるとの判定することにより、取引者の認証の信頼性強化を実現する。

【００５０】＜ステップ８＞認証の判定結果が正しければ、取引き受付けを行い取引を実行する。

【００５１】＜ステップ９＞認証の判定で不正となった場合には、不正使用処理として、予め設定した再試行許可回数を超えた時点で、サーバ側は不正使用者の可能性を防ぐために取引禁止の処理を行う。

【００５２】この取引禁止の処理は、再度「特別な場所」で「安全な通信路」３００によってのみ解除可能なような方法を採用することも可能である。この方法においては、正規の利用者が誤った操作等により不正の判定を受けた場合には、再度前記の「特別な場所」で解除の設定を行うまで取引不能となるが、安全性向上には効果が大きい。

【００５３】認証の判定で不正となった場合以外においては、一旦終了した取引を再開することができ、その場合は再度＜ステップ３＞からのフローに従う。

【００５４】以上説明したように、第１の実施形態に係るセキュリティ強化システムは、通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法において、端末「Ａ」１００が、端末位置を検出する「端末位置検出手段」１２０と、取引許可エリアを設定する「許可エリア設定手段」１３０とを備え、サーバ「Ｂ」２００が、「許可エリア設定手段」１３０により設定された各ユーザの登録エリアを保存する「セキュリティ機能サポート手段」２２０と、「端末位置検出手段」１２０により検出された端末位置が登録エリアにあることを判定する「利用者取引許可エリア判定手段」２３０とを備え、端末位置情報により、利用者認証を補完するようにしているので、端末「Ａ」１００本体に「端末位置検出手段」１２０を備えたことにより、端末内でその現在地の位置データを利用することができ、その位置情報を取引時の認証及び取引データ送信時に付加してサーバ「Ｂ」２００に送信することにより、予め設定した「取引許可エリア」がサーバ「Ｂ」２００のみに知られているため、サーバ「Ｂ」２００は取引端末の位置情報より、その利用者が取引の権利のある人物かどうかの判定が可能となり、可搬端末での利用者認証の信頼性を強化することができる。

【００５５】この方法においては、「安全でない通信路」３１０を用いる取引において、暗号鍵技術によりセキュリティ機能が実現され、更に「暗号鍵」、「ユーザＩＤ」及び「パスワード」等を含む端末本体あるいは利用者カードと端末本体が不正利用者の手に渡った場合においてさえも、前記端末位置情報による認証機能の効果により不正取引を防止することができる。

【００５６】前記、位置検出は上下方向の位置検出も含

むため、取り引き許可エリア設定として建物の何階で使用するか、をも設定可能であり、不正使用者が取引許可の設定の同一建物で不正使用を試みてもフロアが異なれば失敗することとなり、偶然に許可エリア内で不正使用される確率は非常に小さくなる。

【００５７】更に、不正使用者が、真の利用者が予め設定しておいた「再試行許可回数」を越えて試みた場合には、サーバ「Ｂ」２００側で自動的に取引禁止処理を行う設定が可能なため、端末「Ａ」１００が不正使用者の手に渡ったことに気づかずに、利用禁止手続きを行っていなくても、不正に利用される可能性を低減させることができるという優れた効果を奏する。

【００５８】図３は本発明の第２の実施形態に係るセキュリティ強化システムの構成を示す図である。

【００５９】第２の実施形態は、端末の位置検出手段として加速度センサ（運動センサ）を用いた実施形態であり、位置検出情報を用いて取引のセキュリティを強化するシステムは第１の実施形態と同様である。

【００６０】図３において、「可搬型の通信端末本体」４００内部には「６軸の運動センサ」４１０と、その「６軸の運動センサ」４１０の各センサ出力が入力される「端末位置検出手段」１２０とが設置される。

【００６１】上記「６軸の運動センサ」４１０は、直行する３軸の各方向の加速度成分を検出する加速度センサである。加速度を時間軸で積分すると速度成分が得られ、更に速度を時間軸で積分すると変位量が得られるので、高精度でしかも広いダイナミックレンジの加速度の検出がなされれば、その加速度信号をディジタル化して演算することにより、３次元的な変位ベクトルを得ることができる。

【００６２】ところで、端末の向きを常に一定に保ちながら運搬するわけではないため、端末の向きや回転に応じて、瞬時瞬時にその変位ベクトルを補正する必要があり、前記「６軸の運動センサ」の各軸の周りの回転を検出して補正情報として用いるのである。この回転検出情報を、後述する図４に示す「端末位置検出手段」１２０の「３軸回転情報入力手段」１２２に与える。

【００６３】図４は上記「端末位置検出手段」１２０の構成を示すブロック図である。

【００６４】図４において、「端末位置検出手段」１２０は、「変位データ入力手段」１２１、「変位ベクトル計算手段」１２３、「初期値／校正値入力手段」１２４、「メモリ手段」１２５、「現在地座標計算手段」１２６及び「端末現在地３次元座標出力手段」１２７から構成される。

【００６５】図４に示す「端末位置検出手段」１２０において、「変位ベクトル計算手段」１２３は「変位データ入力手段」１２１の情報と「３軸回転情報入力手段」１２２の情報により端末の姿勢と方向の補償を行いながらシステムの備える立体地図との対応が可能な変移ベクトルを計算し、計算した変移ベクトルを「現在地座標計算手段」１２６に出力する。

【００６６】「現在地座標計算手段」１２６では、変位量の方向を含めたベクトルとして、「メモリ手段」１２５に格納されている直前の座標にベクトル的に加算し、累積していくことにより、前記地図上の立体座標系における端末の現在位置座標を算出する。

【００６７】このようにして得られた座標データは「端末現在地３次元座標出力手段」１２７にディジタルデータとして出力される。このディジタルデータを出力する回路は「可搬型端末内」に構造的に隠蔽されており、電気信号として容易には測定できない構造とし、ソフトウエア的にもデータの読みだしを禁止するシステムとする。あるいは、不正なデータ修正を行うことを検出した場合には被認証機能や取引にかかわる機能を破壊し、第１の実施形態で記述した「特別な場所」においてのみ回復させることができるようなシステムを実現することが可能である。

【００６８】こうして得られた、端末位置情報は利用者が意識することなく、認証プロセスにおけるサーバとのディジタル情報授受に自動的に暗号化して送出され、認証装置側で第１の実施形態で説明したように、認証の信頼性を向上させる新たな情報として利用することができる。

【００６９】以上説明したように、第２の実施形態に係るセキュリティ強化システムは、「可搬型の通信端末本体」４００内部に、端末本体の変位を検出する「６軸の運動センサ」４１０を備えているので、端末内に埋め込んだ「６軸の運動センサ」４１０により、システムの有する立体地図の座標系に対応した端末の位置座標を得ることができ、検出された位置情報は自動的に認証プロセスにおいて利用されるため、利用者の操作等の負担を増加させることなく認証の信頼性向上を図ることができる。

【００７０】図５は本発明の第３の実施形態に係るセキュリティ強化システムの構成を示す図である。

【００７１】第３の実施形態は、端末の位置検出手段として、無線電話のサービスゾーンのセル位置情報を用いた実施形態であり、位置情報を用いて取引のセキュリティを強化する方法は第１の実施形態と同様である。

【００７２】この例では自動車電話の一方式を例に説明するが、基本的な概念は他の方式の移動体無線システムにおいても同様である。

【００７３】まず、移動体無線システムにお付るシステムの情報を用いた位置検出について説明する。

【００７４】一般的に、移動体通信システムにおいては、移動機の着呼のために、移動機の着呼時において、移動機に対する一斉呼出しエリアを決定する必要があり、移動機の現在位置を検出して、その位置情報が常に登録されていることが必要である。更に発呼時において

は、在圏無線ゾーン検出がなされるので、より正確な位置情報が得られる。

【００７５】図５は自動車電話のサービスゾーンのセル位置情報を用いた位置検出の概念説明図である。

【００７６】図５において、「Ｐ」は着信制御チャネルを、「Ａ」は発信制御チャネルを表す。また、図中＜ｓ１＞，＜ｓ２＞，…は以下に説明する各ステップの動作＜ステップ１＞，＜ステップ２＞，…にそれぞれ対応する。

【００７７】「自動車電話交換局」を構成する「Ｍ」は「加入者メモリ」を、「ＰＵ」は「「中央演算処理装置」を、「Ｃ」は「通話路装置」をそれぞれ示す。「ホームメモリ局」も「自動車電話交換局」である。

【００７８】次に、位置検出及び登録の動作について説明する。

【００７９】＜ステップ１＞移動機は、位置登録単位である制御ゾーンの、どのゾーンに存在するかを着信制御チャネルで知ることができる。例えば、「制御ゾーンＡ」から「制御ゾーンＢ」に移行した場合、「制御ゾーンＡ」と「制御ゾーンＢ」では、それぞれの着信制御チャネルで知らされている「地域識別コード」が異なることにより知ることができる。

【００８０】＜ステップ２＞移動機は、「制御ゾーンＢ」の着信制御チャネルで報知されている発信制御チャネル情報を受信し、その発信制御チャネルで「位置登録信号」を送出する。「位置登録信号」は同一内容の２フレーム構成である。

【００８１】＜ステップ３＞上記「位置登録信号」は、「無線基地局」を経て「無線回線制御局」まで中継される。「無線回線制御局」では、上記２フレーム構成の「位置登録信号」の各ビットの照合を行い、「位置登録信号」の信頼性を確認する。

【００８２】＜ステップ４＞上記照合後、「位置登録信号」を直属の「自動車電話交換局」に送出する。

【００８３】＜ステップ５＞「自動車電話交換局」は「無線回線制御局」に対して「位置登録確認信号」を送り返すとともに、位置登録してきた移動機の番号から、それが属する自動車電話交換局の「ホームメモリ局」を割りだし、その「ホームメモリ局」に対して「位置登録信号」を転送する。

【００８４】＜ステップ６＞「ホームメモリ局」では、該当移動機加入者のメモリのうち、位置情報部分を書き換える。前記＜ステップ５＞において、自局がホームメモリ局である場合には時局のホームメモリを書き換える。

【００８５】＜ステップ７＞「自動車交換局」から前記「位置登録確認信号」を受信した「無線回線制御局」は、「無線基地局」から「発信制御チャネル」を用いて移動機に対して「位置登録受付信号」を送出し、位置登録を受け付けたことを通知する。

【００８６】＜ステップ８＞この時点で、移動機は初めて、地域識別コードのメモリを書き換え、新しい「制御ゾーン」の着信制御チャネルでの待受けに入る。

【００８７】以上の説明から分かるように、まず、移動機はどの「制御ゾーン」の着信制御チャネルでの待受けに入るかを示す位置情報を移動機側より得ることができるのである。更に、発呼時または通話中の状態においては、移動中の移動機の現在位置をより狭い領域に特定することが可能となる。

【００８８】次に、通話中の状態においての現在位置情報検出について説明する。

【００８９】図６は自動車電話の通話中チャネル切換え制御を説明するための図である。

【００９０】通話中チャネル切換えとは、移動機を搭載している自動車が走行によって通話中に無線ゾーンを移行した場合に、移行先ゾーンで使用している通話チャネルに切換えて通話を継続させることをいう。具体的には、無線ゾーンには明確な境界線があるわけではなく、電波の強度が変動しながら徐々に低下していき、ゾーンの境界付近では両方の基地局の電波が変動しながら重なりあっている。このような変動特性下において、複数ゾーンの中から受信レベルの最も高いゾーンを選択して接続するように動作する。

【００９１】図６において、「移動機」は自動車搭載型の通信装置であり、第１の実施形態で説明した「特別な場所」へも取り外して移動させることができる取引端末である。「移動機」を搭載した自動車は、「無線ゾーンＡ」、「無線ゾーンＢ」、「無線ゾーンＣ」と複数の無線ゾーンにわたって移動する。各無線ゾーンに対応して「無線基地局」が設置されており、各「無線基地局」と「無線回線制御局」、「自動車電話交換局」及び固定網とが通信路で接続されている。

【００９２】次に、通話中チャネル切換え制御の動作について、以下ステップ順に説明する。

【００９３】＜ステップ１１＞「無線ゾーンＡ」で通話していた「移動機」が「無線ゾーンＢ」の方に移動する。

【００９４】＜ステップ１２＞移動機からの通話チャネル受信レベルを常時監視している基地局通話チャネル受信機は、受信レベルが規定値以下に低下したことで移動機が自ゾーンから外へ移動しつつあることを知る。

【００９５】＜ステップ１３＞「無線基地局」は、その通話チャネルのレベル劣化を「無線回線制御局」に通知する。

【００９６】＜ステップ１４＞「無線回線制御局」は「無線ゾーンＡ」及びその周辺の無線ゾーンの基地局に対して、その通話チャネル受信レベル監視を指示する。

【００９７】各基地局は、制御用及び通話用受信機の他に、通話チャネル切換えのための受信レベルの監視を行うＳ／Ｎ監視用受信機を備えており、前記２種類の受信

機の受信周波数が固定であるのに対して、Ｓ／Ｎ監視用受信機は外部からの指令により自動車電話システム内のチャネルのうちの任意のチャネルすなわち隣接セルのチャネルにも切替えることができる。

【００９８】＜ステップ１５＞各基地局は指示に基づいてＳ／Ｎ監視用受信機の受信チャネルをその通話チャネルに切替えて移動機からの電波の受信レベルを測定し、その結果を「無線回線制御局」に報告する。

【００９９】＜ステップ１６＞上記「無線回線制御局」は、最も受信レベルが高かった無線ゾーンを移動機の移動先ゾーンと判断する。他のゾーンへ移動した場合には移動先ゾーンのチャネルに切換えるように「自動車電話交換局」に依頼し、元の基地局Ａの通話チャネルを通して新しい通話チャネルに切替えるように通話中チャネル切替え信号を送出する。

【０１００】＜ステップ１７＞移動機は、指示に従って新しい通話チャネルに切換える。新しい「無線ゾーンＢ」の無線基地局は、移動機との間で新しい通話チャネルの動作を確認して、通話路を「無線ゾーンＢ」の新チャネルへと切換える。

【０１０１】以上の動作における無線ゾーンあるいはチャネルに対応する基地局の位置より、より狭い移動機の位置が特定され、本システムの無線基地局の配置情報より、移動機位置を推定することができる。

【０１０２】なお、詳細説明を省略したが、発呼時においても「無線回線制御局」が、発呼信号に付加された受信レベルを比較することにより、移動機からの信号を最も高いレベルで受信した無線基地局を移動機の「在圏無線ゾーン」と判定して、その無線ゾーンの通話チャネルのうちの使われていないチャネルを選択して、そのチャネルを基地局を介して移動機に指定するように動作する。

【０１０３】これらの位置検出方法は、方向探知技術等による位置検出ではなく、電波の受信レベルによる方法であるので、実際の位置を正確に検出することはできないものの、小さなセルあるいはゾーンを用いるシステムにおいては、十分な検出位置精度を実現することができる。

【０１０４】次に、こうして得られた、端末すなわち移動機の位置情報を第１、第２の実施形態の運動センサによる位置検出の代わりに用いることにより、予め真の利用者が登録しておいたエリア以外での不正取引を禁止し、第１、第２の実施形態と同様に従来の暗号技術のみに頼る場合よりもセキュリティ機能を強化することができる。

【０１０５】以上説明したように、第３の実施形態に係るセキュリティ強化システムは、端末の位置検出を移動体無線通信システムが本来有している移動機位置情報を利用して実現したため、新たに位置検出手段を別に内蔵することなく、第１の実施形態同様のセキュリティ強化

機能を実現して不正利用を防止することができるという優れた効果がある。

【０１０６】図７は本発明の第４の実施形態に係るセキュリティ強化システムの説明図である。

【０１０７】前記第２の実施形態は、端末の位置検出手段として加速度センサを運動センサとして用いた実施形態であり、前記第３の実施形態は移動体無線通信システムの有する移動機位置情報を取り出して用いた例であるが、第４の実施形態においては、運動センサからの検出位置情報と移動体無線通信システムの有する移動機位置情報の両方を用いて取引のセキュリティを更に強化するシステムである。

【０１０８】図７に示す地図状の説明図において、８１～８４及び８５の円状の領域は、前記第３の実施形態で説明した移動体通信システムからの情報により端末位置検出可能な各「無線ゾーン」を示す。

【０１０９】図７においては、８６及び８７を同一平面上に記載しているが、８６は移動先の「特定ゾーン」においてのみ表示及び操作が可能なグラフィック・ユーザ・インタフェースを表し、８７は前記実施形態１で説明した「特別な場所」においてのみ表示及び操作が可能なグラフィック・ユーザ・インタフェースを表す。

【０１１０】例えば、８７においては８５として示されているゾーンの中の８８に示す網掛け部分のエリアを取引許可エリアとする。この図においては８５の外側の領域の図示を省略しているが、実際のユーザ・インタフェースにおいてはサーバ側から周辺を含む地図的なデータが伝送されてきて表示されるので、目的のエリアを容易に確認することができる。

【０１１１】この「特別な場所」で取引を許可する「目的のエリア」を設定することにより、サーバ側に登録する。この登録したエリアの情報は、前記「特定ゾーン」において表示可能なグラフィック・ユーザ・インタフェースにおいては見られず、８６内に示されているように単なる地図表示である。

【０１１２】次に、この「特定ゾーン」と「詳細位置校正」について説明する。

【０１１３】「特定ゾーン」は、前記「特別な場所」において設定した「目的のエリア」を含む無線ゾーンである。移動体通信システムから得られる位置情報のみではこのゾーンの中のどの位置に端末があるか分からず、どの位置に端末があるかまで検出するためには、前記「運動検出センサからの検出位置情報」を利用する。

【０１１４】ここで、「運動検出センサからの検出位置情報」が検出誤差累積により利用不可能と判断した場合は、「詳細位置校正」を行う。

【０１１５】「詳細位置校正」は、前記「特定ゾーン」においてのみ可能とする。これは、既に「ゾーン」精度での位置検出は保証されていること、「目的のエリア」がゾーン内に存在するため精度上有利なこと、真の利用

者の操作場所であること等の理由による。しかも、不正な利用者が「詳細位置校正」を試みるゾーンと一致しない可能性があり、不正な「詳細位置校正」の危険性の低減に有効である。

【０１１６】「詳細位置校正」は、前述のように「特定ゾーン」内の、「目的のエリア」内の特定ポイントにおいて、「詳細位置校正」用のグラフィック・ユーザ・インタフェースを起動し、真の利用者のみが知っている地図上の特定ポイントと前記「運動検出センサからの検出位置情報」に基づいて表示される端末現在地表示を一致させることにより行う。

【０１１７】こうして、「特定ゾーン」内の「目的のエリア」を他のエリアから区別するのに十分な端末位置検出精度が実現され、第１の実施形態で説明した検出端末位置情報による取引のセキュリティ強化が実現できる。

【０１１８】以上説明したように、第４の実施形態に係るセキュリティ強化システムは、端末位置検出手段として、移動体通信システムからの位置情報獲得手段と端末本体の運動センサの両方を備えて構成しているので、運動センサのみでは検出誤差が累積して、正確な位置情報が得られない程移動範囲が大きい場合であっても、移動体無線通信システムによる位置情報より端末のおおまかな位置が、無線ゾーンあるいはセルの大きさの精度で得られ、その中の更に正確な位置検出を運動センサを用いて検出するので、例えば、日本全国を移動したような場合であっても、位置情報によるセキュリティ強化機能の性能が低下することがない。

【０１１９】逆に、運動センサによる位置検出に要求される精度としては、比較的狭い無線ゾーンの範囲を、移動範囲として限定することが可能となって、運動センサによる位置検出手段のコスト低減あるいは検出方法の単純化が可能となる。

【０１２０】更に、本実施形態では、端末のおおまかな位置を移動体無線通信システムによる位置情報より得るようにしているが、必ずしも、実際の取引には移動体無線通信システムの回線を使わなくてもよく、例えば、より安全性が低いと考えられている無線あるいは有線のＬＡＮ接続が利用可能な場合に、そのＬＡＮ接続においても、位置情報による取引のセキュリティ機能強化が実現される。

【０１２１】「特別な場所」で設定した取引を許可する「目的のエリア」に関する情報は、前記「特定ゾーン」における「詳細位置校正」時において、利用者には隠されているため「真の利用者」以外の不正に校正を防止できるという優れた効果がある。

【０１２２】図８は本発明の第５の実施形態に係るセキュリティ強化システムの構成を示す図である。本実施形態に係るセキュリティ強化システムの説明にあたり図１に示すセキュリティ強化システムと同一構成部分には同一符号を付して重複部分の説明を省略する。

【０１２３】第５の実施形態は、移動端末本体に外部からの位置検出システム用の電波を受信する手段を備え、その受信電波を利用して端末位置を検出して得られた位置情報を第１の実施形態と同様のセキュリティ強化に利用する例である。

【０１２４】図８において、「Ａ」は可搬の被認証者の端末５００、「Ｂ」は「Ａ」の利用者及びその他の利用者を認証し、商取引サービスを提供するサーバで２００ある。

【０１２５】上記端末「Ａ」５００は、ＲＳＡ暗号系「認証手段」１１０、「端末位置検出手段」５１０及び「取引許可エリア設定手段」１３０を備えて構成され、「端末位置検出手段」５１０は、「ＧＰＳ受信機」５１１、「受信判定手段」５１２及び「補間手段」５１３を備えている。

【０１２６】本実施形態は、「端末位置検出手段」５１０が、ＧＰＳ（Global PositioningSystem）受信機５１１を備え、ＧＰＳ受信機５１１からの位置情報により端末の現在地を検出する他は第１の実施形態と全く同一である。

【０１２７】衛星からの電波により位置を算出するＧＰＳは広く用いられており、車載用のＧＰＳ受信機により自車の位置とその進路を確認するものについては、例えば、特開昭６０－１５５７３号公報に開示されたものがある。

【０１２８】本実施形態においては、車載用の例のような主に野外で使用する移動端末を想定しており、基本的には「ＧＰＳ受信機」５１１は常に衛星からの「衛星航法電波信号」の受信が可能であるとするが、上記「補間手段」５１３を備えているので、仮に電波受信が不可能な時間的な間隙があっても、端末の移動速度が推定できるため、推定位置あるいは推定位置の範囲を推定して「端末位置情報」として利用することができる。

【０１２９】また、不正利用者が不正な目的で「ＧＰＳ受信機」５１１に電波が到達しない状況をつくりだしたり、あるいは移動環境が原因で受信状況の悪い状態が継続した場合には、上記「受信判定手段」５１２が受信不可状況継続時間から判断して、正確な「端末位置情報」を保持していないとの理由により「認証手段」１１０に対して取引禁止の制御を行う。

【０１３０】「認証手段」１１０は、取引禁止の制御下において、繰り返して取引行為が試みられた場合においては、「認証装置Ｂ」において、第１の実施形態の＜ステップ９＞で述べた場合と同様に、「予め設定した再試行許可回数を超えた時点で、サーバ側は不正使用者の可能性を防ぐために取引禁止の処理を行う。」という設定を行うことも可能である。

【０１３１】以上説明したように、第５の実施形態に係るセキュリティ強化システムは、外部からの信号による位置検出手段として、端末の位置検出にＧＰＳシステム

を利用するようにしているので、端末の位置座標の検出誤差が累積するという問題が全くなく、検出位置の「校正」が不要となる。したがって、利用者にとっての設定負担がなくなり、不正な目的での校正も不可能となるのでセキュリティが強化される。

【０１３２】認証プロセスにおいて授受するディジタルデータに、こうして得られた端末位置情報を利用することにより、利用者認証のセキュリティが強化されることは第１の実施形態同様であるが、「受信判定手段」５１２を設けることにより不正利用者が不正な目的で「ＧＰＳ受信機」５１１の動作不可状態をつくりだしても、不正取引を禁止することができ、不正に繰り返して取引行為が試みられた場合には、認証装置側でも取引禁止の処理の設定ができるので、不正利用者の手に移動端末が渡った場合でも、不正取引を防止できる可能性が大きくなるという優れた効果がある。

【０１３３】図９は本発明の第６の実施形態に係るセキュリティ強化システムの構成を示す図である。本実施形態に係るセキュリティ強化システムの説明にあたり図８に示すセキュリティ強化システムと同一構成部分には同一符号を付して重複部分の説明を省略する。

【０１３４】第６の実施形態は第５の実施形態とほぼ同様の構成であるが、更に「運動センサ」を利用する方法と組み合わせて、「運動センサ」により検出した移動ベクトルにより、「ＧＰＳ受信機」の動作不可状態の移動量を算出し、「補間手段」の補間処理の精度を向上させるようにしたものである。第６の実施形態は、「衛星航法電波」の到達しない所に長時間存在した場合でも、精度よく端末位置を検出することを可能にして、取引を可能とするものである。

【０１３５】図９において、「Ａ」は可搬の被認証者の端末６００、「Ｂ」は「Ａ」の利用者及びその他の利用者を認証し、商取引サービスを提供するサーバで２００ある。

【０１３６】上記端末「Ａ」６００は、ＲＳＡ暗号系「認証手段」１１０、「端末位置検出手段」６１０及び「取引許可エリア設定手段」１３０を備えて構成され、「端末位置検出手段」６１０は、「ＧＰＳ受信機」５１１、「受信判定手段」５１２、「補間手段」５１３及び「運動センサ」６１１を備えている。

【０１３７】すなわち、被認証端末「Ａ」６００の「端末位置検出手段」６１０が「ＧＰＳ受信機」５１１、「受信判定手段」５１２、「補間手段」５１３及び「運動センサ」６１１からなる「変位検出手段」６１０を備える構成である他は、前記第１の実施形態と同一である。

【０１３８】第６の実施形態においても、被認証端末が「ＧＰＳ受信機」５１１を備えているので、前記第５の実施形態と同様に「衛星航法電波信号」により、端末の絶対位置を知ることができる。

【０１３９】前記第５の実施形態は、「衛星航法電波信号」の受信感度が不良な状態では、その受信状態を「受信判定手段」５１２により判定し、「補間手段」５１３において、推定端末移動速度から端末位置の範囲を推定することにより、受信感度が不良な状態が短期間の場合に限って、補間による位置推定により端末位置を知ることができた。

【０１４０】第６の実施形態においては、更に、「運動センサ」６１１による変位検出手段を備えているため、受信感度が不良な状態下にあっても「運動センサ」６１１による変位検出手段により変位を検出することが可能である。この位置検出については、第２の実施形態において、加速度センサ等による「６軸運動センサ」４１０を用いた例により既に説明した。

【０１４１】第６の実施形態は、２種の位置検出手段を備えているため、それらの検出手段の精度と利用可能条件によって、組み合わせ使用の主と従の関係を変えることができる。

【０１４２】まず、「衛星航法電波信号」を常に受信できる環境での使用を重視する場合には、移動端末の位置情報として、第５の実施形態同様、「ＧＰＳ受信機」５１１からの位置情報を用い、受信感度が不良な状態が生じる毎に、受信感度が不良な期間のみの変位を検出し、受信感度が不良な状態が生じる直前の位置を基準として、前記「受信感度が不良な期間のみの変位」をベクトル加算して現在地の座標を算出して用い、検出受信状況が改善するれば直ちに「ＧＰＳ受信機」５１１からの位置情報に切り換えて用いる。

【０１４３】一方、一般的には屋内で使用するが、時々屋外に持ち出して移動させるような場合で、屋内においては受信感度が不良な状態が継続するような場合には、第２の実施形態同様「運動センサ」６１１による変位検出による位置情報を主に用いる。

【０１４４】この場合には、定期的あるいは「衛星航法電波信号」が利用できる状況では積極的に「ＧＰＳ受信機」５１１からの位置情報を、第２の実施形態の説明において説明した図４の「端末位置検出手段」１２０の「初期値／校正値入力手段」１２４への校正位置情報として与えることにより、「運動センサ」６１１による変位検出誤差の累積を防ぐことができる。このようにして、「運動センサ」６１１による変位検出と「ＧＰＳ受信機」５１１からの位置情報を組み合わせることにより、より信頼性のある端末位置検出が可能になる。この位置情報を第１の実施形態で説明した、認証時に授受するディジタルデータに付加するようにすれば、より利用者認証の信頼性を高くすることができる。

【０１４５】以上説明したように、第６の実施形態に係るセキュリティ強化システムは、端末の位置検出にＧＰＳシステムを利用することにより、第５の実施形態同様に検出位置「校正」が不要であり、しかも「運動セン

サ」６１１により「衛星航法電波」の到達しない所での長時間位置検出を可能にしたことにより、利用場所の制限が殆んどなくなり、精度のよい位置情報を得て、取引者の認証における信頼度を強化することができる。

【０１４６】ＧＰＳシステムによる位置検出を主なる位置情報として利用し、「運動センサ」６１１による位置検出を補間的に用いる場合には、「衛星航法電波」の到達しない短期間すなわち狭い移動範囲の変位の検出のために十分な精度があればよく、「運動センサ」６１１による位置検出において高い精度は不要となる。

【０１４７】また、「運動センサ」６１１による位置検出を主なる位置情報として利用し、ＧＰＳシステムを利用して得た位置情報を「運動センサ」６１１による位置検出の絶対位置校正に利用する方法では、常時「ＧＰＳ受信機」を動作させる必要がなく、移動端末の省消費電力化に有効である。

【０１４８】これらの方法を実際的に利用する状況では、例えば、端末を運搬するときは動きが激しいため「運動センサ」６１１による位置検出誤差が生じやすいけれど、運搬中は「衛星航法電波」が利用できるので問題がなく、屋内に入って利用する環境では「衛星航法電波」が利用できないので「運動センサ」６１１に頼ることになるが、この場合は端末が静止している状態で利用するので「運動センサ」６１１による位置検出誤差が累積することがなく、非常に合理的な動作が期待できる。

【０１４９】図１０は本発明の第７の実施形態に係るセキュリティ強化システムの構成を示す図である。本実施形態に係るセキュリティ強化システムの説明にあたり図１に示すセキュリティ強化システムと同一構成部分には同一符号を付して重複部分の説明を省略する。

【０１５０】第７の実施形態は、被認証者の端末が車載用の端末であって、端末位置情報を自動車用のナビゲーションシステムから得ることを特徴とするセキュリティ強化方法である。

【０１５１】図１０において、被認証端末「Ａ」７００は車載用の端末であり、第１の実施形態で説明した「特別な場所」における設定時以外は主に車内で用いる。

【０１５２】被認証端末「Ａ」７００の「端末位置検出手段」１２０は、データ出力ポート７１０を備えた「カー・ナビゲーション・システム端末」７２０に接続される。

【０１５３】「カー・ナビゲーション・システム端末」７２０は、汎用の車両用ナビゲーション装置であり、走行経路や自車の位置と道路地図との対応表示ができる。車両用ナビゲーション装置には、上記の「運動センサ」や「ＧＰＳ」受信機を備えたものや車輪の回転から走行距離を算出するものなどあり、例えば、特開平４－２９７８２１号公報に開示されたものがある。

【０１５４】「カー・ナビゲーション・システム端末」７２０には、車両位置を道路地図の座標に対応付ける「自車の位置」情報を出力するデータ出力ポート７１０を備え、このデータ出力ポート７１０は被認証端末「Ａ」７００の「端末位置検出手段」１２０に接続されている。

【０１５５】以上の構成において、被認証端末「Ａ」７００の「端末位置検出手段」１２０は「カー・ナビゲーション・システム端末」７２０より「自車の位置」情報を受けとるが、汎用のナビゲーション装置からのデータであるので、ナビゲーション装置における地図情報との対応情報を、被認証装置あるいは認証装置における位置情報を表現する座標系で理解することができるように、「端末位置検出手段」１２０が座標対応付けを行う。すなわち、「端末位置検出手段」１２０は自ら位置検出を行う代わりにナビゲーション装置からの自車位置情報を変換することにより端末位置座標を算出する。

【０１５６】こうして得られた端末位置座標を、認証時に授受するディジタル情報に付加することにより、利用者認証の信頼性を高めることができることは第１の実施形態と同様である。

【０１５７】なお、自車位置情報が被認証装置の外から入力できる構造であっても、真の利用者が認証装置に登録している取引許可領域は、第三者には知られていないので不正目的で自車位置情報を入力しようとする試みが成功する確率は非常に低い。

【０１５８】以上説明したように、第７の実施形態に係るセキュリティ強化システムは、端末の位置検出を汎用の「カー・ナビゲーション・システム端末」７２０からの「自車の位置」情報を変換して得ているため、取引用の端末本体に高度の位置検出手段を備える必要がなく、端末単体のコスト低減が可能である。「カー・ナビゲーション・システム端末」７２０からの「自車の位置」情報はその表示によって、自車位置を地図上で確認できるため、位置検出誤りによる誤動作の心配がないという効果を得ることができる。

【０１５９】したがって、上記各実施形態で詳述したように、優れた特長を有する本セキュリティ強化システムを移動体端末における認証方法に利用すれば、被認証端末は、その端末位置を検出し、現在位置情報を利用することができるので、この端末位置情報を、取引時の認証プロセスで授受するディジタルデータに付加することにより、秘密に登録してある取引許可エリア以外における不正取引を防止することができ、暗号技術等を用いた認証機能に加えてセキュリティ機能強化が実現できる。

【０１６０】また、安全でない通信路を用いることにより、認証に用いる秘密情報が第三者に盗まれた場合や、認証に用いる秘密情報を含む端末やカード状のデバイスそのものが第三者の手に渡ってしまった場合でも、位置情報によるセキュリティ機能は有効に機能するため、インターネット等のオープンなネットワークを用いる電子商取引の利用者の認証機能強化に利用することができ

る。

【０１６１】特に、可搬型の端末であって、デバイスそのものが第三者に渡った場合の不正取引を防ぐセキュリティ機能が強化されているので、携帯型の取引端末に利用することができる。

【０１６２】この端末位置情報による利用者認証確度の強化方法は、身体的特徴を利用する、他の一般的な方法よりも融通性があり、心情的な拒絶感を与えることがなく好ましいと考えられる。

【０１６３】なお、上記各実施形態では、被認証端末内に認証に用いる秘密情報を含む例で説明しているが、認証に用いる秘密情報や位置検出手段をカード状のデバイスに実装して、端末と分離・結合できる構成としてもよく、同様なセキュリティ強化効果を得ることができる。

【０１６４】また、上記各実施形態では、ネットワークを介しての用いたセキュリティ強化システムに適用した例について説明したが、通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法には全て適用することができる。

【０１６５】さらに、セキュリティ強化システムという名称に限定されるものではなく、本発明の技術的思想の範囲内であれば認証方法等のように適宜変更することができ、通信システムの一部に組み込まれる態様であってもよいことは言うまでもない。

【０１６６】

【発明の効果】本発明に係るセキュリティ強化システムでは、通信回線を介して授受されるディジタル情報により端末利用者の認証を行う認証方法のセキュリティ強化システムであって、被認証者の装置は、端末位置を検出する端末位置検出手段と、取引許可エリアを設定する許可エリア設定手段とを備え、認証者の装置は、許可エリア設定手段により設定された各ユーザの登録エリアを保存する登録エリア保存手段と、端末位置検出手段により検出された端末位置が登録エリアにあることを判定するエリア判定手段とを備え、端末位置情報により、利用者認証を補完するように構成しているので、不正な利用者による「なり済まし」の危険性を排除して、安全でない通信路を利用する場合においてもセキュリティ機能を格段に強化することができる。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施形態に係るセキュリティ強化システムの構成を示すブロック図である。

【図２】上記セキュリティ強化システムの動作を説明するためのフローチャートである。

【図３】本発明を適用した第２の実施形態に係るセキュリティ強化システムの構成を示す図である。

【図４】上記セキュリティ強化システムの端末位置検出手段の構成を示すブロック図である。

【図５】本発明を適用した第３の実施形態に係るセキュリティ強化システムの位置検出を説明するための図である。

【図６】上記セキュリティ強化システムの自動車電話の通話中チャンネル切換え制御をを説明するための図である。

【図７】本発明を適用した第４の実施形態に係るセキュリティ強化システムを説明するための図である。

【図８】本発明を適用した第５の実施形態に係るセキュリティ強化システムの構成を示すブロック図である。

【図９】本発明を適用した第６の実施形態に係るセキュリティ強化システムの構成を示すブロック図である。

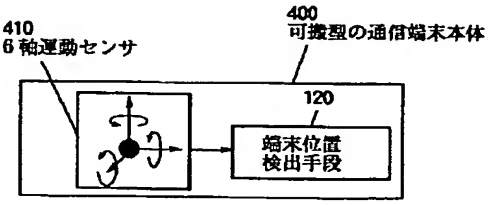
【図１０】本発明を適用した第７の実施形態に係るセキュリティ強化システムの構成を示すブロック図である。

【図１１】ＲＳＡ暗号方式のアルゴリズムを示す図である。

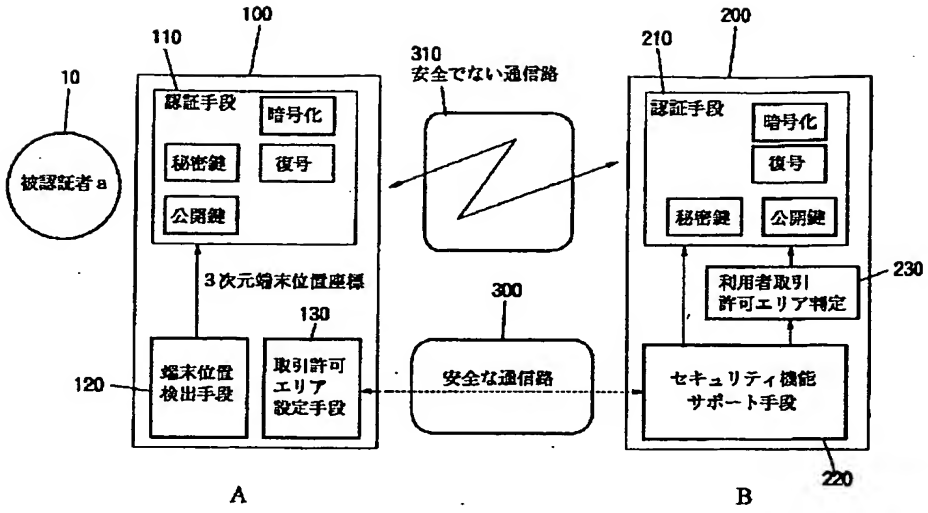
【符号の説明】

１０　認証者ａ、１００，５００，６００，７００　被認証端末「Ａ」（被認証者の装置）、１１０，２１０　「認証手段」、１２０，５１０，６１０　「端末位置検出手段」、１３０　「取引許可エリア設定手段」、２００　サーバ「Ｂ」（認証者の装置）、２２０　「セキュリティ機能サポート手段」（登録エリア保存手段）、２３０　「利用者取引許可エリア判定手段」（エリア判定手段）、３００　「安全な通信路」、３１０　「安全でない通信路」、４００　「可搬型の通信端末本体」、４１０，６１１　「６軸の運動センサ」、５１１　「ＧＰＳ受信機」、５１２　「受信判定手段」、５１３　「補間手段」、７１０　データ出力ポート、７２０　「カー・ナビゲーション・システム端末」

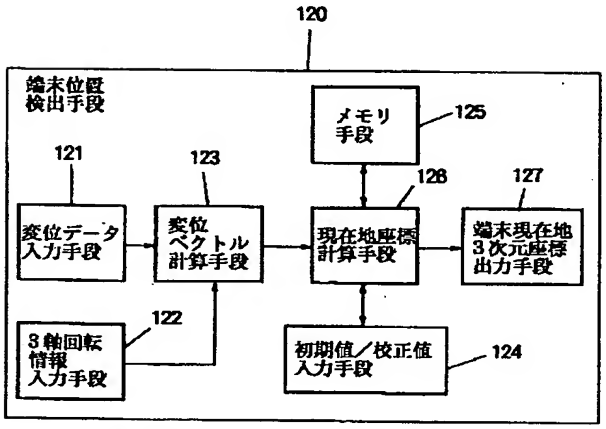
【図３】



【図１】

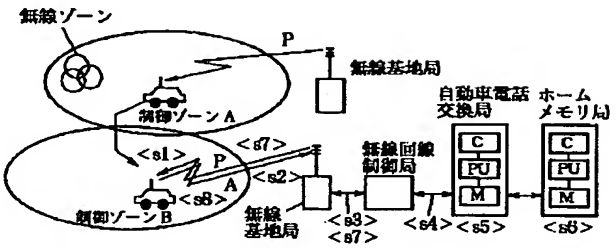


【図４】



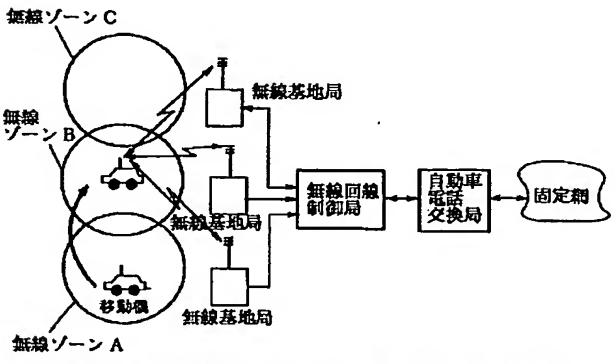
第２の実施形態における端末位置検出手段のブロック図

【図５】



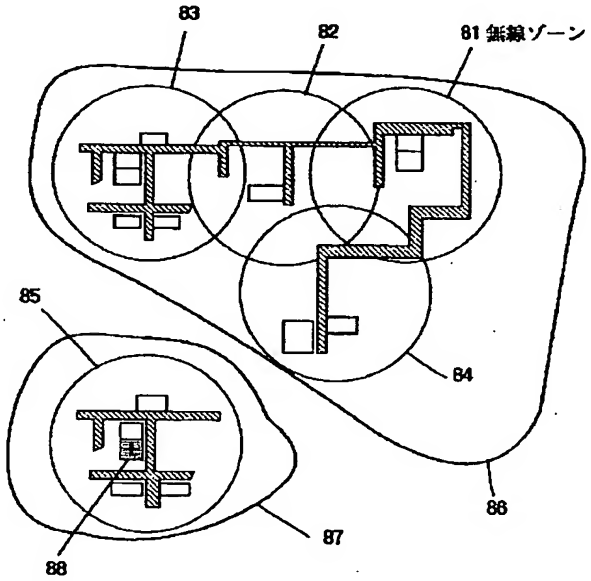
第３の実施形態の位置検出の説明図

【図６】

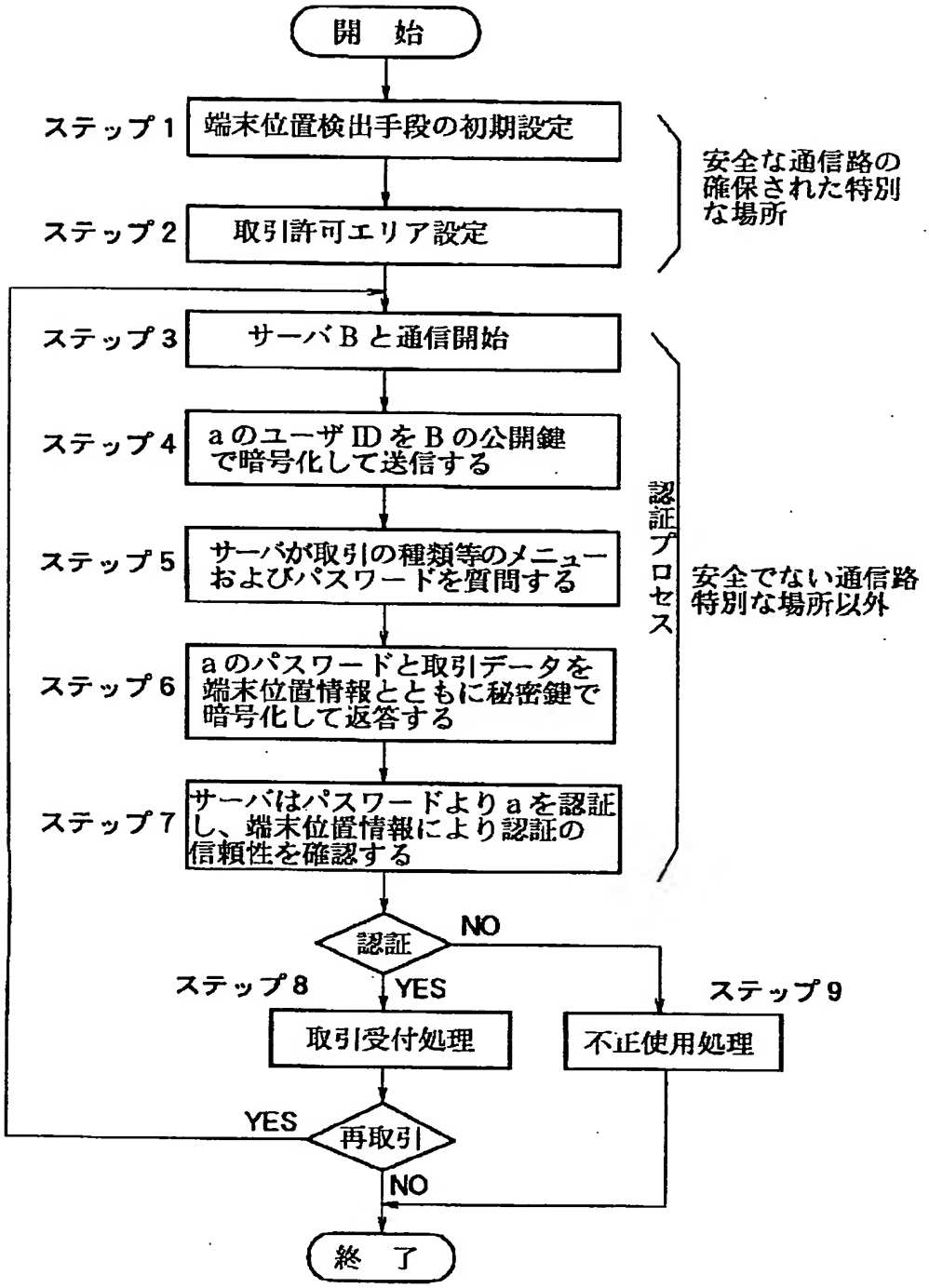


自動車電話の通話中チャネル切換え制御の説明図

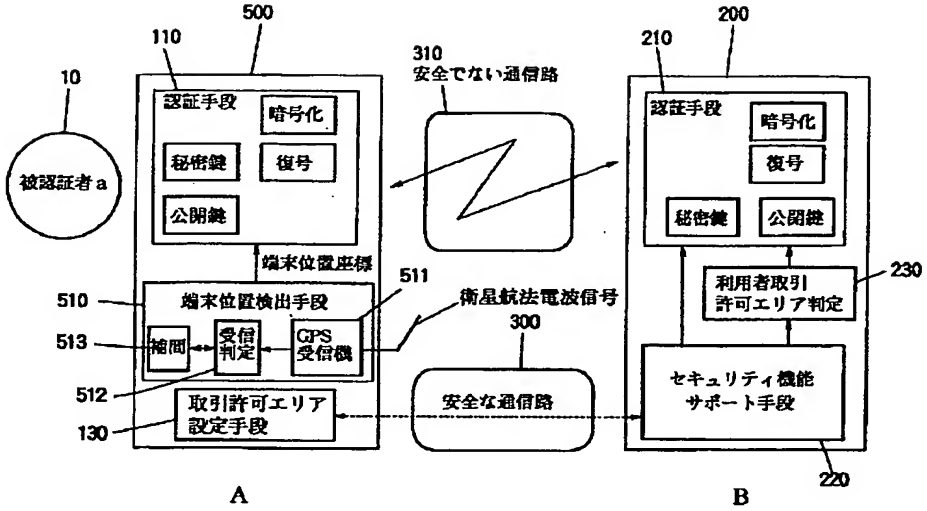
【図７】



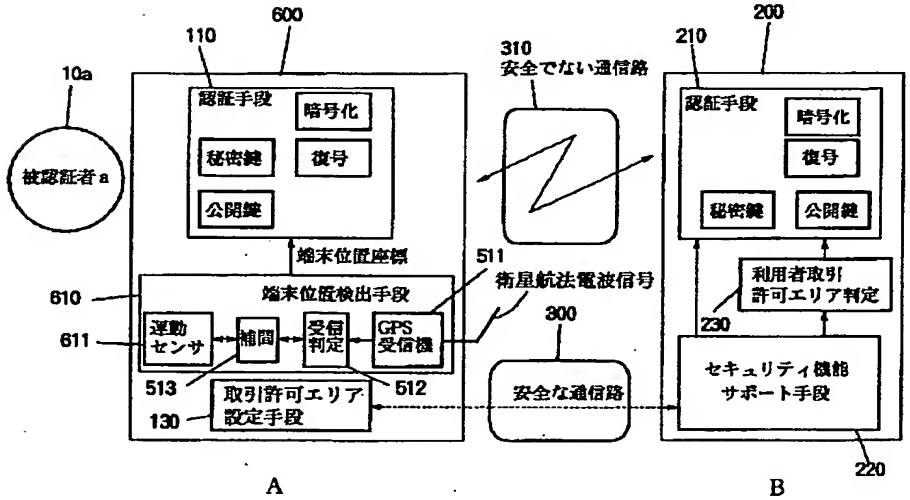
【図２】


開　始
ステップ１
端末位置検出手段の初期設定
ステップ２
取引許可エリア設定
安全な通信路の確保された特別な場所
ステップ３
サーバＢと通信開始
ステップ４
ａのユーザＩＤをＢの公開鍵で暗号化して送信する
ステップ５
サーバが取引の種類等のメニューおよびパスワードを質問する
ステップ６
ａのパスワードと取引データを端末位置情報とともに秘密鍵で暗号化して返答する
ステップ７
サーバはパスワードよりａを認証し、端末位置情報により認証の信頼性を確認する
認証プロセス
安全でない通信路特別な場所以外
認証
NO
YES
ステップ８
ステップ９
取引受付処理
不正使用処理
YES
再取引
NO
終　了

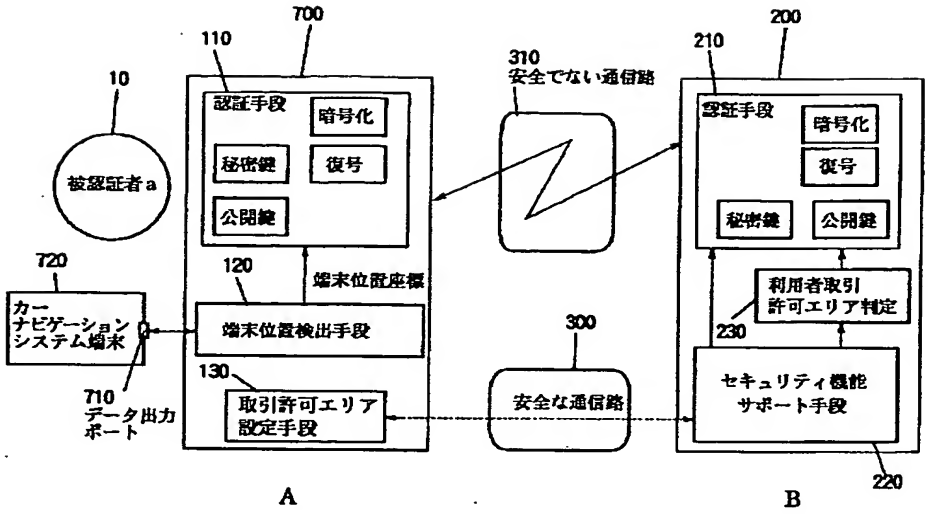
【図８】


500
110
10
認証手段
暗号化
秘密鍵
復号
公開鍵
被認証者a
端末位置座標
510
端末位置検出手段
511
衛星航法電波信号
513
補間
受信判定
GPS受信機
300
512
取引許可エリア設定手段
130
安全な通信路
A
310
安全でない通信路
200
210
認証手段
暗号化
復号
秘密鍵
公開鍵
利用者取引許可エリア判定
230
セキュリティ機能サポート手段
220
B

【図９】


600
110
10a
認証手段
暗号化
秘密鍵
復号
公開鍵
被認証者a
端末位置座標
610
端末位置検出手段
511
衛星航法電波信号
運動センサ
611
補間
受信判定
GPS受信機
300
513
512
取引許可エリア設定手段
130
安全な通信路
A
310
安全でない通信路
200
210
認証手段
暗号化
復号
秘密鍵
公開鍵
利用者取引許可エリア判定
230
セキュリティ機能サポート手段
220
B

【図１０】



【図１１】

暗号化　：　$C=M_e \bmod n$

復号　　：　$M=C^d \bmod n$

ここで

M	：平文
C	：暗号文
e, n	：公開鍵
d	：秘密鍵
p, q	：大きな素数(陰の秘密鍵)
n	：p×q
L	：p−1とq−1の最小公倍数
e	：Lと互いに素な数
d	：[e×d] mod L=1を満たす数

RSA暗号方式のアルゴリズム

フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
G09C	1/00	660		G06F	15/30	340
H04Q	7/36			H04B	7/26	104Z
	7/34					106A
	7/38					109R
				H04L	9/00	673B
						673E
						675B

Japanese Patent Application Laid-Open No. 10-56449

Date of Laid-Open: February 24, 1998

(54) [Title of the Invention] Security Reinforcing System

(57) [Abstract]

[Object] To provide a security reinforcing system which eliminates the possibility of impersonation performed by an unauthorized user and reinforces a security function even when a non-secure communication channel is used.

[Solution] A security reinforcing system using an authentication method for authenticating the user of a terminal by means of digital information which is exchanged via a communication line, wherein a terminal A 100 comprises terminal location detecting means 120 for detecting the location of the terminal and permitted area setting means 130 for setting a transaction permitted area; a server B 200 comprises security function supporting means 220 for storing the registered areas of users which have been set by the permitted area setting means 130 and user transaction permitted area determining means 230 for determining whether the location of a terminal which has been detected by the terminal location detecting means 120 is within the registered area; and authentication of a user is complemented by the terminal location information.

[Claims]

[Claim 1] A security reinforcing system using an authentication method for authenticating the user of a

terminal by means of digital information which is exchanged via a communication line, wherein

the device of one to be authenticated comprises:

terminal location detecting means for detecting the location of the terminal, and

permitted area setting means for setting a transaction permitted area;

the device of one who performs authentication comprises:

registered area storing means for storing the registered areas of users which have been set by the permitted area setting means, and

area determining means for determining whether the location of a terminal which has been detected by the terminal location detecting means falls within the registered area; and

authentication of a user is complemented by the terminal location information.

[Claim 2] A security reinforcing system as described in claim 1, wherein, as the digital information exchanged via a communication line, the terminal location information is encrypted and then transmitted to the device of the one who performs authentication.

[Claim 3] A security reinforcing system as described in claim 1 or 2, wherein the terminal location detecting means has a motion sensor for detecting displacement of a terminal body.

[Claim 4] A security reinforcing system as described in claim 1 or 2, wherein the terminal location detecting means has location information acquiring means for acquiring location information by means of a mobile communication system.

[Claim 5] A security reinforcing system as described in claim 1 or 2, wherein the terminal location detecting means comprises location information acquiring means for acquiring location information by means of a mobile communication system, and a motion sensor for detecting displacement of a terminal body and detects the location of a terminal based on location information acquired by the location information acquiring means and displacement data obtained by the motion sensor.

[Claim 6] A security reinforcing system as described in claim 1 or 2, wherein the terminal location detecting means has location detecting means for detecting location information by means of an external signal.

[Claim 7] A security reinforcing system as described in any one of claims 1, 2, and 6, further comprising correction means for correcting terminal location information obtained by the terminal location detecting means.

[Claim 8] A security reinforcing system as described in claim 1 or 2, wherein the terminal location detecting means comprises location detecting means for detecting location information by means of an external signal, means for detecting displacements by means of a motion sensor, and

evaluation means for evaluating the receiving condition of an external signal and corrects the terminal location information by use of displacement data obtained by the displacement detecting means based on evaluation made by the evaluating means.

[Claim 9] A security reinforcing system as described in any one of claims 6, 7, and 8, wherein the external signal is a GPS radio signal.

[Claim 10] A security reinforcing system as described in claim 1 or 2, wherein the security reinforcing system limits a communication channel used for registering areas in the registered area storing means.

[Claim 11] A security reinforcing system as described in claim 1 or 2, wherein the device of one who performs authentication has means for registering the number of times one to be authenticated is allowed to retry a request for authentication and performs a transaction prohibiting process when the number of times the area determining means determines that location information attached to digital information exchanged on request for authentication fails to match area information registered in advance exceeds the number of allowable retries.

[Claim 12] A security reinforcing system as described in claim 1 or 2, wherein the terminal of one to be authenticated is a car-mounted terminal which acquires terminal location information through a car-mounted navigation system.

[Claim 13] A security reinforcing system as described in

claim 1 or 2, wherein the terminal of one to be authenticated or one who performs authentication comprises detected location correcting means for correcting a location detected by the terminal location detecting means, and limiting means for limiting at least one of the setting of the detected terminal location correcting means, the setting of the permitted area setting means, and a location of the terminal in which the permitted area setting means is allowed to display data.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to a security reinforcing system for network security, and more particularly to a security reinforcing system for authenticating the user of a mobile terminal.

[0002]

[Prior Art]

In recent years, electronic commerce via a network has become a reality. When a fixed, closed public circuit is used, the security of a transaction is protected by means of a user ID and a password, or an account number and a personal identification number. However, particularly when an open network such as the Internet is used, the security of information and authentication of a user are becoming big concerns.

[0003]

Further, when a business transaction conducted via a network can be performed anywhere by means of a mobile terminal or the like, preventing an unauthorized user from breaking into a place where a terminal is installed can no longer be said to guarantee security of the transaction; and authentication of a user is an essential technique for realizing secure on-line commerce.

[0004]

A representative example of an authentication method is a method using an RSA encryption system. An example of the method is described in "Information Security Technique and Service in Network," Television Institute Journal Vol. 49, No. 12, pp. 1,567 to 1,571 (1995).

[0005]

In the above literature, a brief description of the RSA encryption system and a description of an information protection system using the RSA encryption system are presented.

[0006]

Cryptographic algorithms are roughly classified into two systems; that is, common key encryption and public key encryption, and RSA is a representative example of public key encryption. In common key encryption, an encryption key and a decryption key are the same, and a sender and a receiver perform encryption and decryption quickly with the keys maintained secret between the sender and the receiver. Meanwhile, in public key encryption typified by the RSA, an

encryption key and a decryption key are different, anybody can encrypt a communication by means of the public encryption key of a receiver, and the communication is decrypted by means of a private key owned only by a legitimate receiver. The system has a characteristic such that when the order of encryption and decryption is reversed, only one who possesses a private key can perform private conversion (digital signature) and anybody who knows the public key of the owner of the private key can perform public conversion (verification of signature).

[0007]

This characteristic is used to perform authentication of a receiver and for verification that the communication has been conducted safely and securely.

[0008]

"RSA" of the RSA public encryption system is formed by the first letters of the names of three developers in MIT; i.e., Rivest, Shamir, and Adleman. The algorithm of the RSA encryption system is shown in Fig. 11.

[0009]

In the system, two types of encryption keys are prepared. One of the keys is called a private key and maintained only by its owner. The other key is called a public key and is passed to one with whom the owner intends to communicate.

[0010]

In Fig. 11, d represents a private key, and (e, n) represent public keys. Text encrypted by means of the

private key can be decrypted only by means of the corresponding public keys, whereas text encrypted by means of the public keys can be decrypted only by means of the corresponding private key. In functions of encryption and decryption, "a mod n" represents the remainder when a is divided by n.

[0011]

The RSA encryption system will be specifically described with reference to an exemplary case where a user A transmits a message to a user B.

[0012]

It is assumed that A has the public key of B and B has the public key of A. A first method is a method in which A performs encryption by use of the public key of B, and a second method is a method in which A performs encryption by use of his own private key.

[0013]

In the first method, since a message transmitted by A can be decrypted only by means of the private key of B, the confidentiality of the information can be protected from a third person. Meanwhile, in the second method, since a message transmitted from A to B can be prepared only by means of the private key of A, it is guaranteed that the transmitter is A, and it can be assumed that the content of the message has not been tampered with.

[0014]

Since authentication of the user A can be performed by

the second method, it can be used as digital signature. Further, since the message transmitted from A to B can be decrypted by means of the public key of A, the second method can also protect data in combination with the first method.

[0015]

The security of the system consists depends on difficulty in performing large-scale factorization into prime factors when n is large, and since a decryption method other than a method comprising trying all possible keys has not yet been found, the system is considered one of the most reliable public key encryption systems.

[0016]

[Problems to be solved by the Invention]

However, the system is not completely free from the possibility that a third person finds an algorithm for creating a private key from a public key or obtains the private key. The shorter a private key is, the easier it is to break the private key. This is particularly problematic when the system is used via a non-secure communication channel. Further, even if the possibility is theoretically decreased, the possibility that a third person who has acquired a user card or terminal incorporating a private key makes unauthorized use of the user card or terminal by impersonating the rightful owner of the card or terminal cannot be prevented.

[0017]

Particularly, when a private key has portability as in

the case of a user card or portable terminal, the possibility that a user card or portable terminal falling into the hands of a hostile third person still remains even if the possibility that the information is stolen via a network is eliminated.

[0018]

An object of the present invention is to provide a security reinforcing system which eliminates the possibility of impersonation performed by an unauthorized user and reinforces a security function even when a non-secure communication channel is used.

[0019]

[Means for Solving the Problems]

The security reinforcing system according to the present invention is a security reinforcing system using an authentication method for authenticating the user of a terminal by means of digital information which is exchanged via a communication line, wherein the device of one to be authenticated comprises terminal location detecting means for detecting the location of the terminal and permitted area setting means for setting a transaction permitted area; the device of one who performs authentication comprises registered area storing means for storing the registered areas of users which have been set by the permitted area setting means and area determining means for determining whether the location of a terminal which has been detected by the terminal location detecting means falls within the

registered area; and authentication of a user is complemented by the terminal location information.

[0020]

Further, as the digital information exchanged via a communication line, the terminal location information may be encrypted and then transmitted to the device of the one who performs authentication. The terminal location detecting means may have a motion sensor for detecting displacement of a terminal body.

[0021]

Further, the terminal location detecting means may have location information acquiring means for acquiring location information by means of a mobile communication system. The terminal location detecting means may comprise location information acquiring means for acquiring location information by means of a mobile communication system, and a motion sensor for detecting displacement of a terminal body and may detect the location of a terminal based on location information acquired by the location information acquiring means and displacement data obtained by the motion sensor.

[0022]

Further, the terminal location detecting means may have location detecting means for detecting location information by means of an external signal. The system may also have correction means for correcting terminal location information obtained by the terminal location detecting means.

[0023]

Further, the terminal location detecting means may comprise location detecting means for detecting location information by means of an external signal, means for detecting displacements by means of a motion sensor, and evaluation means for evaluating the receiving condition of an external signal and may correct the terminal location information by use of displacement data obtained by the displacement detecting means based on evaluation made by the evaluating means. The external signal may be a GPS radio signal.

[0024]

Further, the above security reinforcing system may limit a communication channel used for registering areas in the registered area storing means.

[0025]

Further, the device of one who performs authentication may have means for registering the number of times one to be authenticated is allowed to retry a request for authentication and perform a transaction prohibiting process when the number of times the area determining means determines that location information attached to digital information exchanged on request for authentication fails to match area information registered in advance exceeds the number of allowable retries.

[0026]

Further, the terminal of one to be authenticated may be a car-mounted terminal which acquires terminal location

information through a car-mounted navigation system.

[0027]

Further, the terminal of one to be authenticated or one who performs authentication may comprise detected location correcting means for correcting a location detected by the terminal location detecting means, and limiting means for limiting at least one of the setting of the detected terminal location correcting means, the setting of the permitted area setting means, and a location of the terminal in which the permitted area setting means is allowed to display data.

[0028]

[Embodiments of the Invention]

A security reinforcing system according to the present invention can be applied to a security reinforcing system that can be used for reinforcing the function of authenticating a user of electronic commerce using an open network such as the Internet.

[0029]

Fig. 1 is a block diagram showing the configuration of the security reinforcing system according to a first embodiment of the present invention.

[0030]

In Fig. 1, A represents a portable terminal 100 of one to be authenticated (device of one to be authenticated), and B represents a server 200 (device of one who performs authentication) which authenticates the user of A and other users and provides business transaction service.

[0031]

First, the terminal A 100 and the server B 200 have RSA encryption system authentication means 110 and 210, respectively, which are of the aforementioned prior art.

[0032]

Further, the terminal A 100 comprises terminal location detecting means 120 for detecting the current location of the terminal constantly by detecting the location of a sensor terminal which detects the direction, position, and three-dimensional motion of the terminal, and transaction permitted area setting means 130 which includes a graphic user interface function which makes it possible to associate a location of the terminal and a transaction permitted area with a three-dimensional map.

[0033]

The three-dimensional map as used herein refers to a map which enables recognition of the planer lay-out of each building as well as floor levels thereof.

[0034]

Meanwhile, the server B 200 comprises security function supporting means (registered area storing means) 220 for securely storing data on the password and transaction permitted area of each user and referring to the data at the time of authentication, and user transaction permitted area determining means (area determining means) 230 for determining, on the basis of the data, whether a transaction is to be permitted.

[0035]

The terminal A 100 and the server B 200 communicate with each other via a network. More specifically, they can communicate with each other by means of a secure communication channel 300 whose security is guaranteed with respect to a special location. As for other places, the terminal A 100 and the server B 200 use a non-secure communication channel 310 for the sake of convenience.

[0036]

The secure communication channel 300 as used herein refers to a line which is generally immune to phone tapping and through which an unauthorized third person cannot carry out communication by use of the same address or telephone number without permission, or a line which is open but whose security is guaranteed to be of the same level as described above by employment of a security technique such as cryptography. Meanwhile, the non-secure communication channel 310 is a line through which it is technically possible for a third person having special knowledge and equipment to steal communication data.

[0037]

Although Fig. 1 shows only one to be authenticated a 10 as a user, in the general case a plurality of similar users and a plurality of terminals exist, and the one to be authenticated a 10 represents one of the terminals. In addition, it is also possible that a plurality of users physically share the same terminal with which each of the

users can be authenticated separately. Depending on the constitution of the users, it may also be possible to use different cryptographic keys.

[0038]

In this case, although the configuration of Fig. 1 shows cryptographic keys incorporated into the terminal, the keys can be incorporated into an IC card or user card which can be detached from a terminal.

[0039]

Next, the operation of a security reinforcing system having the above configuration will be described.

[0040]

Fig. 2 is a flowchart for illustrating the operation of a security reinforcing system having the configuration of Fig. 1. The operation will be described following the steps constituting the operation.

[0041]

<STEP 1> In Fig. 1, the one to be authenticated a 10 who is the user of the terminal A 100 effects the initial setting of the terminal location detecting means 120 of the terminal A 100. In the initial setting, the current location and direction of the terminal are adjusted to the coordinates and direction of a special location on a map of the system. The one to be authenticated a 10 is permitted to make the initial setting of the terminal location detecting means 120 of the terminal A 100 only when the one to be authenticated a 10 is authenticated in the special location by the server B 200 via

the secure communication channel 300. Thereby, there can be eliminated the possibility of a third person making improper setting for the purpose of conducting illegitimate transactions. It is assumed that the secure communication channel 300 is available between the server B 200 and such a special location.

[0042]

<STEP 2> By use of the graphic user interface of the transaction permitted area setting means 130 of the terminal A 100, the one to be authenticated a 10 who is the user of the terminal A 100 registers in the security function supporting means 220 of the server B 200 an area in which a business transaction with the terminal A 100 is permitted. In general, the registration process is conducted in a special location. It is assumed that the secure communication channel 300 is also available between the server B 200 and the special location.

[0043]

<STEP 3> A case where the terminal A 100 is brought in areas other than the special location set in advance in the <STEP 2> will be described as an example hereinafter. To conduct a transaction by means of not the secure communication channel 300 but the non-secure communication channel 310, the terminal A 100 firstly starts to communicate with the server B 200.

[0044]

<STEP 4> The one to be authenticated a 10 transmits

his/her own user ID code by use of the public key of the server B 200.

[0045]

<STEP 5> The server B 200 identifies the transmitted user ID code by use of the private key of the server B 200. Although the user who has transmitted the user ID code cannot be authenticated at this point, there is no possibility of the user ID code having been stolen by a third person, since nobody but the server knows the private key of the server B 200.

[0046]

The server B 200 inquires the identified user about his/her password and the type of transaction.

[0047]

<STEP 6> The one to be authenticated a 10 transmits his/her own password and transaction data after encrypting the password and data by use of a private key (in this case, the private key of the terminal A 100). At this point, the location information of the terminal A 100 is attached automatically and encrypted and transmitted together with the password and transaction data.

[0048]

In addition to encryption performed by use of the private key of the server B 200, further encryption is performed by use of the public key of the server B 200. This eliminates the possibility that the password, transaction data, and location information are stolen by a third person

who has acquired the public key of the one to be authenticated a 10.

[0049]

<STEP 7> The server B 200 authenticates the one to be authenticated a 10 and confirms that the transaction data have not been subjected to tampering, by decrypting the password, transaction data, and location information by use of the public key of the user identified in the above <STEP 5> (that is, the public key of the terminal A 100). In addition, the server B 200 also checks that the location information attached automatically by the location information detecting means 120 is included in the transaction permitted area registered in advance so as to determine that the one to be authenticated a 10 is a valid transactor, thereby improving the reliability of authentication of a transactor.

[0050]

<STEP 8> When the result of the authentication is valid, the server B 200 accepts and processes the transaction.

[0051]

<STEP 9> When the result of the authentication is invalid, the server performs, as an unauthorized use process, a transaction prohibiting processing for preventing possible unauthorized use of the terminal by an unauthorized person when authentication is retried in excess of the number of allowable retries set in advance.

[0052]

To cancel the prohibition of transactions, a method may be used in which the terminal A 100 can be freed from the prohibition of transactions only in the special location via the secure communication channel 300. In this method, when an authorized user is determined to be an unauthorized user by a misoperation or the like, the authorized user is unable to conduct a transaction until the prohibition on transactions is cleared in the special location. This measure is highly effective for improving security.

[0053]

Unless the result of the authentication is invalid, a transaction terminated once can be resumed, following the flow from <STEP 3> inclusive.

[0054]

As described above, the security reinforcing system according to the first embodiment employs an authentication method for authenticating the user of a terminal by means of digital information which is exchanged via a communication line. In the system, the terminal A 100 comprises the terminal location detecting means 120 for detecting the location of the terminal and the permitted area setting means 130 for setting a transaction permitted area; the server B 200 comprises the security function supporting means 220 for storing the registered areas of users which have been set by the permitted area setting means 130 and the user transaction permitted area determining means 230 for determining whether the location of a terminal which has been detected by the

terminal location detecting means 120 falls within the registered area; and authentication of a user is complemented by the terminal location information. The terminal A 100 incorporates the terminal location detecting means 120 so that location data on its current location can be used within the terminal. The location information is attached to authentication and transaction data upon transmission of the authentication and transaction data for conducting a transaction, and transmitted to the server B 200. Since only the server B 200 knows a preset transaction permitted area, the server B 200 can determine, on the basis of the location information of the transaction terminal, whether the user of the terminal is qualified to conduct a transaction. Thus, the system can reinforce the reliability of user authentication with a portable terminal.

[0055]

In this method, a security function is realized by a cryptographic key technique in a transaction using the non-secure communication channel 310. Further, even when a terminal incorporating cryptographic keys, a user ID, and a password or a pair consisting of a terminal and a user card incorporating cryptographic keys, a user ID, and a password falls into the hands of an unauthorized user, an illegitimate transaction can be prevented by virtue of the effect of the authentication function using the terminal location information.

[0056]

The above location detection includes location detection in a vertical direction. Thus, which floor of a building on which a terminal is to be used can also be set as a transaction permitted area setting. Therefore, even if an unauthorized user attempts to make unauthorized use of the terminal in the same building, he fails to do so if he makes the attempt on a floor different from the one on which the terminal is allowed to be used, and the probability that the unauthorized user happens to make an unauthorized use of the terminal in the permitted area becomes very small.

[0057]

In addition, the server B 200 can be set to perform a transaction prohibition process automatically when an unauthorized user has made a retry in excess of the number of allowable retries set in advance by an authorized user. Therefore, the security reinforcing system exhibits the excellent effect that it can reduce the possibility of unauthorized use of a terminal A 100 when the user of the terminal A 100 is unaware that the terminal has fallen into the hands of an unauthorized user and therefore does not go through a procedure for prohibiting use of the terminal A 100.

[0058]

Fig. 3 is a diagram showing the configuration of a security reinforcing system according to a second embodiment of the present invention.

[0059]

The second embodiment is an embodiment using an

acceleration sensor (motion sensor) as terminal location detecting means, and the system which reinforces the security of a transaction by use of detected location information is the same as that of the first embodiment.

[0060]

In Fig. 3, within a portable communication terminal body 400, a six-axis motion sensor 410 and terminal location detecting means 120 into which are input the sensor outputs of the six-axis motion sensor 410 are provided.

[0061]

The above six-axis motion sensor 410 is an acceleration sensor which detects acceleration components in the directions of three axes intersecting at right angles. Integration of acceleration with respect to time yields a velocity component, and integration of velocity with respect to time yields a displacement. Therefore, if acceleration is detected with high accuracy and a wide dynamic range, the acceleration signal can be digitized and calculated to produce a three-dimensional displacement vector.

[0062]

Meanwhile, since a user does not carry a terminal with its orientation maintained constant at all times, its displacement vector must be corrected from moment to moment according to the orientation and rotation of the terminal, and the rotation about each axis of the above six-axis motion sensor is detected for use as correction information. The detected rotation information is provided to the 3-axis

rotation information inputting means 122 of the terminal location detecting means 120, which is shown in Fig. 4 and will be described later.

[0063]

Fig. 4 is a block diagram showing the configuration of the above terminal location detecting means 120.

[0064]

In Fig. 4, the terminal location detecting means 120 comprises displacement data inputting means 121, displacement vector calculating means 123, initial value/correction value inputting means 124, memory means 125, current location coordinates calculating means 126, and terminal current location three-dimensional coordinates outputting means 127.

[0065]

In the terminal location detecting means 120 shown in Fig. 4, the displacement vector calculating means 123 calculates a displacement vector which can be associated with a three-dimensional map provided in the system while compensating the position and direction of a terminal on the basis of information from the displacement data inputting means 121 and information from the 3-axis rotation information inputting means 122 and outputs the calculated displacement vector to the current location coordinates calculating means 126.

[0066]

The current location coordinates calculating means 126 adds the calculated displacement vector to the immediately

preceding coordinates stored in the memory means 125 as a vector including the direction of displacement and accumulates the coordinates to thereby calculate the coordinates of the current location of the terminal on the three-dimensional coordinates on the above map.

[0067]

The thus obtained coordinates data are output to the terminal current location three-dimensional coordinates outputting means 127 as digital data. A circuit to output the digital data is concealed structurally in the portable terminal, has such a structure that it cannot be readily measured by means of electrical signals and is a system which prohibits data from being read by means of software. Alternatively, it is also possible to realize a system which destroys a function used for being authenticated and a transaction related function when detecting unauthorized data modification and can recover the functions only in the special location described in the first embodiment.

[0068]

The thus obtained terminal location information is encrypted and transmitted automatically, without a user being aware of it, when the terminal exchanges digital information with the server in an authentication process and can be used by the device which performs authentication as new information which can improve the reliability of authentication as described in the first embodiment.

[0069]

As described above, in the security reinforcing system according to the second embodiment, the portable communication terminal body 400 incorporates the six-axis motion sensor 410 which detects displacements of the terminal body. The six-axis motion sensor 410 incorporated into the terminal provides location coordinates of the terminal which correspond to the coordinate system on a three-dimensional map provided in the system. The detected location information is automatically used in an authentication process. Thus, the security reinforcing system can improve the reliability of authentication without increasing burdens involved in the operation by a user and the like.

[0070]

Fig. 5 is a diagram showing the configuration of a security reinforcing system according to a third embodiment of the present invention.

[0071]

The third embodiment is an embodiment using cell location information of service zones of a radio telephone as terminal location detecting means, and a method of reinforcing the security of a transaction by use of location information is the same as the first embodiment.

[0072]

Although the present embodiment will be described with reference to one automobile telephone system as an example, the basic concept of the present embodiment is the same in other mobile body radio systems.

[0073]

Firstly, location detection using system information in a mobile radio system will be described.

[0074]

In general, in a mobile communication system, when mobile units are called, an area in which mobile units are located must be determined in order for the mobile units to receive a call, and therefore the current locations of the mobile units must be detected and registered constantly. Further, radio zones in which the mobile units are present are detected when the mobile units originate a call. Consequently, more accurate location information can be obtained.

[0075]

Fig. 5 is a conceptual diagram for illustrating location detection using cell location information of service zones of an automobile telephone.

[0076]

In Fig. 5, P represents a reception control channel, and A represents a transmission control channel. Further, <s1>, <s2>, ... <sN> in Fig. 5 correspond to the operations of <STEP 1>, <STEP 2>, ... <STEP N> to be described below, respectively.

[0077]

In an automobile telephone exchange, M represents a subscriber memory, PU represents a central processing unit, and C represents a channel device. A home memory station is

also an automobile telephone exchange.

[0078]

Next, operations in location detection and location registration will be described.

[0079]

<STEP 1> A mobile unit can know in which control zone it is present by means of a reception control channel. The location of a mobile unit is registered by the control zone. For example, when a mobile body moves from a control zone A to a control zone B, the mobile body can know the switch of the control zones because area identification codes provided via the reception control channels of the control zone A and the control zone B are different.

[0080]

<STEP 2> The mobile unit receives transmission control channel information provided via the reception control channel of the control zone B and transmits a location registration signal via the transmission control channel. The location registration signal comprises two frames having the same content.

[0081]

<STEP 3> The above location registration signal is passed to a radio line control station via a radio base station. At the radio line control station, each bit of the location registration signal comprising two frames is verified so as to check the reliability of the location registration signal.

[0082]

<STEP 4> After the verification, the radio line control station transmits the location registration signal to a corresponding automobile telephone exchange.

[0083]

<STEP 5> The automobile telephone exchange not only transmits a location registration confirmation signal to the radio line control station but also determines a home memory station of an automobile telephone exchange to which the mobile unit belongs, based on the number of the mobile unit which has transmitted the location registration signal, and transfers the location registration signal to the home memory station.

[0084]

<STEP 6> The home memory station rewrites the location information stored in the memory of the subscriber of the mobile unit. In the above <STEP 5>, when the automobile telephone exchange which transmits the location registration confirmation signal to the radio line control station is the automobile telephone exchange to which the mobile unit belongs, the home memory station of the automobile telephone exchange rewrites the location information stored in the memory of the subscriber of the mobile unit.

[0085]

<STEP 7> After receiving the above location registration confirmation signal from the automobile telephone exchange, the radio line control station transmits a location

registration acceptance signal from the radio base station to the mobile unit via the transmission control channel to thereby notify the mobile unit that the location registration has been accepted.

[0086]

<STEP 8> At this point, the mobile body rewrites the area identification code in the memory for the first time and assumes a standby status with the reception control channel of the new control zone.

[0087]

As can be understood from the above description, a mobile unit can first provide location information indicating in which control zone the mobile unit assumes a standby status with the transmission control channel of the control zone. In addition, the current location of a mobile unit on the move can be limited to a narrower area at the time of making a telephone call or during a telephone conversation.

[0088]

Next, detection of the current location information of a mobile unit during a telephone conversation will be described.

[0089]

Fig. 6 is a diagram for illustrating mid-call channel switching control of an automobile telephone.

[0090]

The mid-call channel switching refers to switching to a channel used in a newly entered zone when an automobile having a mobile unit moves from one radio zone to another

radio zone during a telephone conversation so as to continue the telephone conversation. To be more specific, there is no distinct boundary between radio zones. The intensity of radio waves in a radio zone gradually decreases, while fluctuating, toward the boundary of the zone, and the radio waves from the base stations of adjacent areas are superimposed on each other near the boundary between the areas while fluctuating. Under such a fluctuation characteristic, the system operates such that it selects a zone with the highest reception level from a plurality of zones and connects the mobile unit to its base station.

[0091]

In Fig. 6, a mobile unit is a communication device which is mountable on an automobile and is a transaction terminal which can be detached from the automobile and brought in the special location as described in the first embodiment. An automobile having the mobile unit mounted thereon moves over a plurality of radio zones, i.e., a radio zone A, a radio zone B, and a radio zone C. A radio base station is provided for each of the radio zones, and the radio base stations, a radio line control station, an automobile telephone exchange, and a fixed network are connected via a channel.

[0092]

Next, the operation of the mid-call channel switching control will be described in terms of steps.

[0093]

<STEP 11> A mobile unit which is in the middle of having

a telephone conversation in the radio zone A moves into the radio zone B.

[0094]

<STEP 12> A base station communication channel receiver which constantly monitors the reception level of the communication channel from the mobile unit becomes aware of the movement by sensing that the reception level has become lower than or equal to a predetermined value.

[0095]

<STEP 13> The radio base station notifies the radio line control station of the reduction in the level of the communication channel.

[0096]

<STEP 14> The radio line control station directs the base stations of the radio zone A and its surrounding radio zones to monitor the reception level of the communication channel.

[0097]

Each of the base stations has, in addition to a control receiver and a communication receiver, an S/N monitoring receiver that monitors a reception level for switching communication channels. While the received frequencies of the aforementioned two types of receivers are fixed, the S/N monitoring receiver can be switched to any channel out of channels in an automobile telephone system; that is, even to the channel of an adjacent cell, by an externally provided direction.

[0098]

<STEP 15> The base stations each switch the reception channel of the S/N monitoring receiver to the communication channel on the basis of the direction so as to measure the reception level of radio waves from the mobile unit and report the result to the radio line control station.

[0099]

<STEP 16> The above radio line control station determines that a radio zone with the highest reception level is the radio zone into which the mobile station has moved. When the mobile unit has moved into another zone, the radio line control station requests the automobile telephone exchange to switch to the channel of the zone into which the mobile station has moved and transmits a mid-call channel switching signal so as to urge the mobile unit to switch to the new communication channel, via the communication channel of the base station A where the mobile unit has been originally present.

[0100]

<STEP 17> The mobile unit switches to the new communication channel according to the direction. The radio base station of the radio zone B into which the mobile unit has moved checks the operation of the new communication channel to the mobile unit and switches to the new channel of the radio zone B.

[0101]

The locations of the base stations corresponding to the

radio zones or channels in the above operations determine a narrower location of the mobile unit, and the location of the mobile unit can be estimated by the location information of the radio base stations of the present system.

[0102]

In addition, although detailed descriptions have been omitted, even when the mobile unit is to originate a call, the radio line control station compares reception levels attached to call signals with each other, determines that a radio base station that has received the signal from the mobile station at the highest level is a radio zone in which the mobile unit is present, selects an unused channel out of communication channels of the radio zone, and directs the mobile unit to switch to the selected channel via the radio station.

[0103]

These location detecting methods rely not on a direction finding technique but on reception levels of radio waves. Therefore, although they cannot detect the actual location of a mobile unit accurately, they can still achieve location detection with satisfactory accuracy in a system using small cells or zones.

[0104]

Further, use of the thus obtained location information of the terminal, i.e., mobile unit, in place of the location detection by the motion sensor in the first and second embodiments can prevent unauthorized transactions in areas

other than the area registered in advance by an authorized user and, as in the case of the first and second embodiments, can achieve a more reinforced security function than can the conventional cryptographic technology alone.

[0105]

As described above, the security reinforcing system according to the third embodiment achieves detection of the location of a terminal by use of mobile unit location information intrinsic to a mobile radio communication system. Therefore, the security reinforcing system of the third embodiment has the excellent effect that it can achieve the same security reinforcing function as that of the first embodiment without newly incorporating another location detecting means to prevent unauthorized use of a terminal.

[0106]

Fig. 7 is a diagram for illustrating a security reinforcing system according to a fourth embodiment of the present invention.

[0107]

Whereas the second embodiment is an embodiment using an acceleration sensor as a motion sensor serving as terminal location detecting means and the third embodiment is an embodiment in which mobile unit location information is extracted from a mobile radio communication system and used, the fourth embodiment is a system which further reinforces the security of transactions by use of both location information detected by a motion sensor and mobile unit

location information of a mobile radio communication system.

[0108]

In the explanatory map-like drawing shown in Fig. 7, circular zones 81 to 85 represent the radio zones which have been described in connection with the third embodiment and in which the location of a terminal can be detected on the basis of information from a mobile communication system.

[0109]

In Fig. 7, although 86 and 87 are drawn in the same plane, reference numeral 86 indicates a graphic user interface that can be displayed and operated only in a specific zone into which a mobile unit moves from a radio zone, and reference numeral 87 indicates a graphic user interface that can be displayed and operated only in the special location described in the first embodiment.

[0110]

For example, it is assumed that the shaded area 88 in the zone 85 in the graphic user interface 87 is a transaction permitted area. Although the surroundings of the zone 85 are not shown in Fig. 7, in reality, map data including the zone's surroundings are transmitted from a server and displayed on the user graphic interface. Thus, the target area can be found readily.

[0111]

The target area in which a transaction is permitted is set in the special location so as to register the target area in the server. Information about the registered area cannot

be seen in the user graphic interface 86 that can be displayed in the specific zone and merely a portion of the map is displayed.

[0112]

Next, the specific zone and detailed location correction will be described.

[0113]

The specific zone is a radio zone including the target area set in the special location. Since the location of a terminal in the zone cannot be known only by means of location information obtained from a mobile communication system, the location information detected by a motion detection sensor is used to detect the location of the terminal in the zone.

[0114]

When the location information detected by a motion detection sensor is determined to be unusable due to cumulative detection errors, detailed location correction is performed.

[0115]

The detailed location correction can be performed only in the above specific zone. The reasons for this are, for example, that the accuracy of location detection in the zone is already insured; this is advantageous in terms of accuracy since the target area is included in the zone; and the zone is a zone where an authorized user performs the detailed location correction. In addition, it may be the case that

the specific zone does not coincide with a zone where an unauthorized user attempts to perform the detailed location correction. Therefore, it is effective for reducing the possibility of unauthorized detailed location correction.

[0116]

The detailed location correction comprises activating the graphic user interface for the detailed location correction at a specific point in the target area within the specific zone as described above and that coincides to a specific point on the map which is known only to an authorized user with the current location of a terminal which is displayed on the basis of the location information detected by a motion detection sensor.

[0117]

Thus, terminal location detection accuracy sufficient to distinguish the target area within the specific zone from other areas is achieved, and the security reinforcement of transactions by use of detected terminal location information as described in the first embodiment can be achieved.

[0118]

As described above, the security reinforcing system according to the fourth embodiment has both location information acquiring means of a mobile communication system and a motion sensor of a terminal serving as terminal location detecting means. Therefore, even when a moving range is so big that accurate location information cannot be obtained by the motion sensor alone due to cumulative

detection errors, the approximate location of the terminal can be obtained in a size of a radio zone or cell from the location information obtained from the mobile radio communication system, and more accurate location of the terminal is then detected by use of the motion sensor. Consequently, even when, for example, the user of the terminal travels across Japan while carrying the terminal, the performance of the security reinforcing function does not deteriorate.

[0119]

Meanwhile, accuracy required for location detection by means of the motion sensor is such that a relatively narrow radio zone range can be limited as a moving range and a reduction in the costs of the location detecting means and simplification of the detection method by use of the motion sensor can be achieved.

[0120]

In addition, although in the present embodiment the approximate location of a terminal is obtained from location information from a mobile radio communication system, a line of the mobile radio communication system does not necessarily have to be used in actual transactions. For example, when wireless or wired LAN access considered less secure is available, reinforcement of the security function of transactions by use of location information is achieved even in the case of LAN access.

[0121]

Information about the target area which has been set in the special location and in which a transaction is permitted is concealed from users at the time of implementation of the detailed location correction in the specific zone. Therefore, the present embodiment has the excellent effect of preventing those who are not an authorized user from performing unauthorized detailed location correction.

[0122]

Fig. 8 is a diagram showing the configuration of a security reinforcing system according to a fifth embodiment of the present invention. In the following description of the security reinforcing system according to the present embodiment, elements which are identical with those of the security reinforcing system shown in Fig. 1 are denoted by the same reference numerals, and repeated descriptions thereof are omitted.

[0123]

The fifth embodiment is an embodiment in which radio waves received by a mobile terminal having means for receiving external radio waves for a location detection system are used to detect the location of the terminal which is then used for security reinforcement, as in the first embodiment.

[0124]

In Fig. 8, A represents a portable terminal 500 of one to be authenticated, and B represents a server 200 which authenticates the user of the terminal A 500 and other users

and provides business transaction service.

[0125]

The terminal A 500 comprises RSA encryption system authentication means 110, terminal location detecting means 510, and transaction permitted area setting means 130. The terminal location detecting means 510 comprises a GPS receiver 511, reception determining means 512, and interpolation means 513.

[0126]

The present embodiment is exactly the same as the first embodiment, except that the terminal location detecting means 510 has the GPS (Global Positioning System) receiver 511 and detects the current location of a terminal on the basis of location information obtained from the GPS receiver 511.

[0127]

GPS, which calculates a position by means of radio waves from satellites, is widely used. An example of GPS used by a car-mounted GPS receiver to check the location and traveling direction of the automobile is disclosed in Japanese Patent Application Laid-Open No. 15573/1985.

[0128]

The present embodiment contemplates a mobile terminal which is mainly used outdoors, as in the case of the example of the car-mounted GPS receiver. Basically, the GPS receiver 511 can receive a satellite navigation radio wave signal from a satellite at any time. However, even if there is a time interval during which the GPS receiver 511 cannot receive

radio waves, the GPS receiver 511 can estimate the moving speed of the terminal since it has the interpolation means 513 and can estimate and use an estimation location or a range of the estimation location as terminal location information.

[0129]

Further, when an unauthorized user creates the situation in which radio waves cannot reach the GPS receiver 511 for an unauthorized purpose or poor reception of radio waves ascribable to a traveling environment continues, the reception determining means 512 determines this condition from the duration during which reception of radio waves is impossible and places the authentication means 110 under the control of transaction prohibition for the reason that accurate terminal location information is not available.

[0130]

When a transaction is attempted repeatedly with the authentication means 110 under the control of transaction prohibition, the authentication system B can perform a transaction prohibition process for eliminating a chance of an unauthorized use of a terminal when the number of times a transaction has been retried exceeds the preset number of allowable retries, as described in <STEP 9> of the first embodiment.

[0131]

As described above, since the security reinforcing system according to the fifth embodiment uses GPS for

detecting the location of a terminal as means for detecting a location by means of external signals, the security reinforcing system is free from the problem that errors in detecting the location coordinates of a terminal are accumulated, and correction of a detected location is not necessary. Consequently, a user is freed from the burden of effecting settings, and correction for an unauthorized purpose cannot be performed, thereby reinforcing security.

[0132]

As in the first embodiment, the thus obtained terminal location information is used as digital data to be exchanged in an authentication process to reinforce the security of user authentication. However, the provision of the reception determining means 512 can prohibit an unauthorized transaction even when an unauthorized user creates for an unauthorized purpose the situation in which the GPS receiver 511 cannot be operated, and the authentication system can also prohibit a transaction when the unauthorized transaction is attempted repeatedly. Therefore, the security reinforcing system according to the fifth embodiment has the excellent effect of increasing the possibility of preventing an unauthorized transaction when a mobile terminal falls into the hands of an unauthorized user.

[0133]

Fig. 9 is a diagram showing the configuration of a security reinforcing system according to a sixth embodiment of the present invention. In the following description of

the security reinforcing system according to the present embodiment, elements which are identical with those of the security reinforcing system shown in Fig. 8 are denoted by the same reference numerals, and repeated descriptions thereof are omitted.

[0134]

The configuration of the sixth embodiment is the same as that of the fifth embodiment, except that, in combination with the method using a motion sensor, a displacement amount of the GPS receiver in an inoperable state is calculated from a displacement vector detected by the motion sensor to thereby improve the accuracy of the interpolation process by the interpolation means. The sixth embodiment is an embodiment which makes it possible to detect the accurate location of a terminal so as to enable a user to perform a transaction even when the user carrying the terminal is present in an area where satellite navigation radio waves cannot reach the terminal for a long period of time.

[0135]

In Fig. 9, A represents a portable terminal 600 of one to be authenticated, and B represents a server 200 which authenticates the user of the terminal A 600 and other users and provides business transaction service.

[0136]

The terminal A 600 comprises RSA encryption system authentication means 110, terminal location detecting means 610, and transaction permitted area setting means 130. The

terminal location detecting means 610 comprises a GPS receiver 511, reception determining means 512, interpolation means 513, and a motion sensor 611.

[0137]

That is, the present embodiment is exactly the same as the first embodiment, except that the terminal location detecting means 610 of the terminal A 600 to be authenticated comprises the GPS receiver 511, the reception determining means 512, the interpolation means 513, and displacement detecting means 610 comprising the motion sensor 611.

[0138]

As in the case of the fifth embodiment, in the sixth embodiment a terminal to be authenticated also has the GPS receiver 511. Therefore, the absolute location of the terminal can be known by means of a satellite navigation radio wave signal as in the case of the fifth embodiment.

[0139]

In the fifth embodiment, when the reception of a satellite navigation radio wave signal is poor, the reception is determined by the reception determining means 512, and the location range of a terminal is estimated from an estimated traveling speed of the terminal by the interpolation means 513. Thereby, the location of the terminal can be known by location estimation by interpolation, but only when the duration of the poor reception is short.

[0140]

Meanwhile, the sixth embodiment additionally has the

displacement detecting means comprising the motion sensor 611. Therefore, even when the reception of a satellite navigation radio wave signal is poor, displacements can be detected by the displacement detecting means comprising the motion sensor 611. This location detection has already been described in the second embodiment by use of the example in which the six-axis motion sensor 410 comprising an acceleration sensor is used.

[0141]

Since the sixth embodiment has two location detecting means, it may assign higher priority to one of them over the other according to the accuracies and usable conditions of the detecting means.

[0142]

In a case where use of a mobile terminal under the circumstances where the terminal can receive a satellite navigation radio wave signal at any time is considered important, location information from the GPS receiver 511 is used as the location information of the terminal as in the case of the fifth embodiment. Every time poor reception of the signal occurs, a displacement during the poor reception period is detected. The displacement, in vector form, is added to the location immediately before the occurrence of the poor reception period to thereby calculate and use the coordinates of the current location of the terminal. Upon restoration of the reception of the signal, use of location information from the GPS receiver 511 is resumed.

[0143]

In contrast, in a case where a terminal is generally used indoors but is sometimes used outdoors and carried around, when poor reception of the satellite navigation radio wave signal continues indoors, location information based on displacement detection by means of the motion sensor 611 is mainly used, as in the case of the second embodiment.

[0144]

In this case, location information from the GPS receiver 511 can be provided to the initial value/correction value inputting means 124 of the terminal location detecting means 120 of Fig. 4 which has been described in connection with the second embodiment, periodically or aggressively under the circumstances where the satellite navigation radio wave signal can be used to prevent accumulation of errors in detecting displacements by the motion sensor 611. Thus, a combination of displacement detection by the motion sensor 611 and location information from the GPS receiver 511 provides more reliable terminal location detection. Attachment of the location information to the digital data exchanged at the time of authentication as described in the first embodiment further improves the reliability of user authentication.

[0145]

As described above, the security reinforcing system according to the sixth embodiment uses the GPS for detecting the location of a terminal, thereby requiring no correction

of a detected location as in the case of the fifth embodiment. Further, use of the motion sensor 611 makes it possible to detect the location of a terminal which is present in an area where satellite navigation radio waves do not reach the terminal over a long time period. Thereby, a terminal can be used almost anywhere, and accurate location information can be obtained to thereby improve the reliability of transactor authentication.

[0146]

When a location detected by the GPS is used as main location information and a location detected by the motion sensor 611 is used as supplemental location information, accuracy of location detection should be sufficient to detect a displacement during a short period when satellite navigation radio waves do not reach a terminal; i.e., a displacement within a narrow moving range. Thus, location detection by means of the motion sensor 611 does not require high accuracy.

[0147]

Meanwhile, in the case of a method in which a location detected by the motion sensor 611 is used as main location information and location information obtained by means of the GPS is used for correction of an absolute location detected by the motion sensor 611, the GPS receiver does not have to be kept in action. Therefore, the method is effective in reducing power consumed by a mobile terminal.

[0148]

When these methods are actually used for detecting the location of a terminal carried around outdoors, for example, errors in location detection by the motion sensor 611 are liable to occur, since the terminal does not remain in the same position when carried around. However, this is not problematic, since satellite navigation radio waves can be used when the terminal is carried around. In contrast, when the terminal is used indoors, detection of the location of the terminal relies on the motion sensor 611, since satellite navigation radio waves cannot be used indoors. In this case, since the terminal is used in a fixed position, errors in location detection by the motion sensor 611 are not accumulated, and therefore a very reasonable operation can be expected.

[0149]

Fig. 10 is a diagram showing the configuration of a security reinforcing system according to a seventh embodiment of the present invention. In the following description of the security reinforcing system according to the present embodiment, elements which are identical with those of the security reinforcing system shown in Fig. 1 are denoted by the same reference numerals, and their repeated descriptions are omitted.

[0150]

The seventh embodiment is a security reinforcing method in which the terminal of one to be authenticated is a car-mounted terminal and terminal location information is

obtained from a car navigation system.

[0151]

In Fig. 10, a terminal A 700 to be authenticated is a car-mounted terminal and is used mainly in a car, except for the time when the setting is made in the special location as described in the first embodiment.

[0152]

A terminal location detecting means 120 of the terminal A 700 to be authenticated is connected to a car navigation system terminal 720 having a data output port 710.

[0153]

The car navigation system terminal 720 is a general-purpose car navigation device and is capable of displaying a road map corresponding to the traveling path and the location of an automobile having the terminal mounted thereon. Illustrative examples of car navigation systems include one having the above motion sensor and/or GPS receiver, one which calculates a traveling distance from the rotations of wheels, and one disclosed in Japanese Patent Application Laid-Open No. 297821/1992.

[0154]

The car navigation system terminal 720 has the data output port 710 that outputs information about the location of the automobile that associates the location of the automobile to corresponding coordinates on a road map. The data output port 710 is connected to the terminal location detecting means 120 of the terminal A 700 to be authenticated.

[0155]

In the above configuration, the terminal location detecting means 120 of the terminal A 700 to be authenticated receives information about the location of the automobile from the car navigation system terminal 720. However, since the information is data obtained from the general-purpose navigation device, the terminal location detecting means 120 associates map information in the navigation device with the coordinate system for showing location information in the device to be authenticated or in a device which performs authentication, so as to determine the location of the automobile on the coordinate system. That is, rather than detecting the location of the automobile by itself, the terminal location detecting means 120 converts the location information of the automobile which is obtained from the navigation device into terminal location coordinates.

[0156]

The thus obtained terminal location coordinates can be attached to digital information exchanged at the time of authentication to thereby improve the reliability of user authentication as in the first embodiment.

[0157]

Further, even when the location information of the automobile can be input by means of devices other than the device to be authenticated, the probability that a third person succeeds in inputting the location information of the automobile for an unauthorized purpose is very low, since a

transaction permitted area registered in the device which performs authentication by an authorized user is not known to the third person.

[0158]

As described above, in the security reinforcing system according to the seventh embodiment, the location of a terminal is obtained by conversion of information about the location of an automobile having the terminal mounted thereon which is obtained from the general-purpose car navigation system terminal 720. Therefore, sophisticated location detecting means does not need to be incorporated into the terminal for conducting a transaction, thereby reducing costs per terminal. The information about the location of the automobile which is obtained from the car navigation system terminal 720 can be displayed on a map so as to check the location of the automobile on the map, thereby obviating concern about a malfunction caused by errors in location detection.

[0159]

Thus, as described in detail in the above embodiments, when the present security reinforcing system having excellent characteristics is used as an authentication method in a mobile terminal, the terminal to be authenticated can detect its location and use information about its current location. Attachment of the terminal location information to digital data exchanged in an authentication process upon transaction can prevent an unauthorized transaction attempted in areas

other than a secretly registered transaction permitted area and reinforce a security function in combination with an authentication function using cryptography or the like.

[0160]

Further, use of a non-secure communication channel may results in a case in which secret information used in authentication or a terminal or card device containing the secret information is stolen by a third person. Even in such a case, since a security function using location information functions effectively, the system can be used for reinforcing the function of authenticating a user in electronic commerce using an open network such as the Internet.

[0161]

Particularly, since a portable terminal incorporating the system has a reinforced security function of preventing an unauthorized transaction when the device itself falls into the hands of a third person, the portable terminal can be used as a portable transaction terminal.

[0162]

The method for reinforcing the accuracy of user authentication by use of terminal location information is considered more versatile than other commonly used methods using physical characteristics and is also considered preferable, since it does not make a user feel rejected.

[0163]

Further, although the example in which secret information to be used for authentication is incorporated

into a terminal to be authenticated has been described in the above embodiments, the secret information to be used for authentication or location detecting means may be incorporated into a card device which can be attached to and detached from a terminal. This configuration can also give the same security reinforcing effect.

[0164]

Further, in the example, the present invention is applied to a security reinforcing system used via a network. However, the present invention can be applied to all authentication methods comprising authenticating the user of a terminal by use of digital information exchanged via a communication channel.

[0165]

In addition, the present invention is not limited by the name "security reinforcing system." Needless to say, its designation can be altered to authentication method or the like as appropriate within the technical principle of the present invention, and the present invention may be incorporated into a portion of a communication system.

[0166]

[Effects of the Invention]

The security reinforcing system according to the present invention is a security reinforcing system using an authentication method for authenticating the user of a terminal by means of digital information which is exchanged via a communication line, wherein the device of one to be

authenticated comprises terminal location detecting means for detecting the location of the terminal and permitted area setting means for setting a transaction permitted area; the device of one who performs authentication comprises registered area storing means for storing the registered areas of users which have been set by the permitted area setting means and area determining means for determining whether the location of a terminal which has been detected by the terminal location detecting means falls within the registered area; and authentication of a user is complemented by the terminal location information. Therefore, the possibility of impersonation performed by an unauthorized user can be eliminated, and a security function can be significantly reinforced even when a non-secure communication channel is used.

[Brief Description of the Drawings]

[Fig. 1] A block diagram showing the configuration of a security reinforcing system according to a first embodiment of the present invention.

[Fig. 2] A flowchart for illustrating the operation of the security reinforcing system of the first embodiment.

[Fig. 3] A block diagram showing the configuration of a security reinforcing system according to a second embodiment of the present invention.

[Fig. 4] A block diagram showing the configuration of the terminal location detecting means of the security reinforcing system of the second embodiment.

[Fig. 5] A diagram for illustrating location detection by a security reinforcing system according to a third embodiment of the present invention.

[Fig. 6] A diagram for illustrating mid-call channel switching control of an automobile telephone performed by the security reinforcing system of the third embodiment.

[Fig. 7] A diagram for illustrating a security reinforcing system according to a fourth embodiment of the present invention.

[Fig. 8] A block diagram showing the configuration of a security reinforcing system according to a fifth embodiment of the present invention.

[Fig. 9] A block diagram showing the configuration of a security reinforcing system according to a sixth embodiment of the present invention.

[Fig. 10] A block diagram showing the configuration of a security reinforcing system according to a seventh embodiment of the present invention.

[Fig. 11] A diagram showing an algorithm of an RSA encryption system.

[Description of Reference Numerals]

10 one to be authenticated a

100, 500, 600, 700 terminal to be authenticated A (device of one to be authenticated)

110, 210 authentication means

120, 510, 610 terminal location detecting means

130 transaction permitted area setting means

200 server B (device of one to perform authentication)

220 security function supporting means (registered area storing means)

230 user transaction permitted area determining means (area determining means)

300 secure communication channel

310 non-secure communication channel

400 portable communication terminal body

410, 611 six-axis motion sensor

511 GPS receiver

512 reception determining means

513 interpolation means

710 data output port

720 car navigation system terminal

FIG. 1

10 ONE TO BE AUTHENTICATED a

110 AUTHENTICATION MEANS

A PRIVATE KEY

B PUBLIC KEY

C ENCRYPTION

D DECRYPTION

E THREE-DIMENSIONAL TERMINAL LOCATION COORDINATES

120 TERMINAL LOCATION DETECTING MEANS

130 TRANSACTION PERMITTED AREA SETTING MEANS

310 NON-SECURE COMMUNICATION CHANNEL

300 SECURE COMMUNICATION CHANNEL

210 AUTHENTICATION MEANS

230 USER TRANSACTION PERMITTED AREA DETERMINING MEANS

220 SECURITY FUNCTION SUPPORTING MEANS

FIG. 2

A START

STEP 1 MAKE INITIAL SETTING OF TERMINAL LOCATION DETECTING MEANS

STEP 2 SET TRANSACTION PERMITTED AREA

STEP 3 START COMMUNICATION WITH SERVER B

STEP 4 ENCRYPT USER ID OF a WITH PUBLIC KEY OF B AND TRANSMITS THE ID

STEP 5 THE SERVER INQUIRES OF MENUS SUCH AS TYPE OF TRANSACTION AND PASSWORD

STEP 6 ENCRYPT THE PASSWORD OF a, TRANSACTION DATA, AND

TERMINAL LOCATION INFORMATION WITH PRIVATE KEY AND TRANSMIT THEM

STEP 7 THE SERVER AUTHENTICATES a BY THE PASSWORD AND VERIFIES RELIABILITY OF THE AUTHENTICATION BY THE TERMINAL LOCATION INFORMATION

B AUTHENTICATED ?

STEP 8 ACCEPT AND PROCESS TRANSACTION

STEP 9 PERFORM UNAUTHORIZED USE PROCESS

C RETRY TRANSACTION ?

D END

E SPECIAL LOCATION WITH SECURE COMMUNICATION CHANNEL

F AREAS OTHER THAN SPECIAL LOCATION, WITH NON-SECURE COMMUNICATION CHANNEL

G AUTHENTICATION PROCESS

FIG. 3

410 SIX-AXIS MOTION SENSOR

400 PORTABLE COMMUNICATION TERMINAL BODY

120 TERMINAL LOCATION DETECTING MEANS

FIG. 4

BLOCK DIAGRAM OF THE TERMINAL LOCATION DETECTING MEANS OF THE SECOND EMBODIMENT

120 TERMINAL LOCATION DETECTING MEANS

121 DISPLACEMENT DATA INPUTTING MEANS

122 3-AXIS ROTATION INFORMATION INPUTTING MEANS

123 DISPLACEMENT VECTOR CALCULATING MEANS

124 INITIAL VALUE/CORRECTION VALUE INPUTTING MEANS

125 MEMORY MEANS

126 CURRENT LOCATION COORDINATES CALCULATING MEANS

127 TERMINAL CURRENT LOCATION THREE-DIMENSIONAL COORDINATES OUTPUTTING MEANS

FIG. 5

DIAGRAM FOR ILLUSTRATING LOCATION DETECTION IN THE THIRD EMBODIMENT

A RADIO ZONE

B CONTROL ZONE A

C CONTROL ZONE B

D RADIO BASE STATION

E RADIO LINE CONTROL STATION

F AUTOMOBILE TELEPHONE EXCHANGE

G HOME MEMORY STATION

FIG. 6

DIAGRAM FOR ILLUSTRATING MID-CALL CHANNEL SWITCHING CONTROL OF AUTOMOBILE TELEPHONE

A RADIO ZONE A

B RADIO ZONE B

C RADIO ZONE C

D MOBILE UNIT

E RADIO BASE STATION

F RADIO LINE CONTROL STATION

G AUTOMOBILE TELEPHONE EXCHANGE

H FIXED NETWORK

FIG. 7

81 RADIO ZONE

FIG. 8

10 ONE TO BE AUTHENTICATED

110 AUTHENTICATION MEANS

A PRIVATE KEY

B PUBLIC KEY

C ENCRYPTION

D ENCRYPTION

E TERMINAL LOCATION COORDINATES

510 TERMINAL LOCATION DETECTING MEANS

511 GPS RECEIVER

512 RECEPTION DETERMINING MEANS

513 INTERPOLATION MEANS

130 TRANSACTION PERMITTED AREA SETTING MEANS

310 NON-SECURE COMMUNICATION CHANNEL

F SATELLITE NAVIGATION RADIO WAVES SIGNAL

300 SECURE COMMUNICATION CHANNEL

210 AUTHENTICATION MEANS

230 USER TRANSACTION PERMITTED AREA DETERMINING MEANS

220 SECURITY FUNCTION SUPPORTING MEANS

FIG. 9

10 ONE TO BE AUTHENTICATED

110 AUTHENTICATION MEANS

A PRIVATE KEY

B PUBLIC KEY

C ENCRYPTION

D DECRYPTION

TERMINAL LOCATION COORDINATES

610 TERMINAL LOCATION DETECTING MEANS

511 GPS RECEIVER

512 RECEPTION DETERMINING MEANS

513 INTERPOLATION MEANS

611 MOTION SENSOR

130 TRANSACTION PERMITTED AREA SETTING MEANS

310 NON-SECURE COMMUNICATION CHANNEL

F SATELLITE NAVIGATION RADIO WAVES SIGNAL

300 SECURE COMMUNICATION CHANNEL

210 AUTHENTICATION MEANS

230 USER TRANSACTION PERMITTED AREA DETERMINING MEANS

220 SECURITY FUNCTION SUPPORTING MEANS

FIG. 10

10 ONE TO BE AUTHENTICATED a

110 AUTHENTICATION MEANS

A PRIVATE KEY

B PUBLIC KEY

C ENCRYPTION

D DECRYPTION

E TERMINAL LOCATION COORDINATES

120 TERMINAL LOCATION DETECTING MEANS

720 CAR NAVIGATION SYSTEM TERMINAL

710 DATA OUTPUT PORT

130 TRANSACTION PERMITTED AREA SETTING MEANS

310 NON-SECURE COMMUNICATION CHANNEL

300 SECURE COMMUNICATION CHANNEL

210 AUTHENTICATION MEANS

230 USER TRANSACTION PERMITTED AREA DETERMINING MEANS

220 SECURITY FUNCTION SUPPORTING MEANS

FIG. 11

A ENCRYPTION

B DECRYPTION

C WHERE

D ALGORITHM OF RSA ENCRYPTION SYSTEM

M: ORDINARY TEXT

C: ENCRYPTED TEXT

e, n: PUBLIC KEYS

d: PRIVATE KEY

p, q: LARGE PRIME NUMBERS (HIDDEN PRIVATE KEYS)

n: p x q

L: LEAST COMMON MULTIPLE OF p-1 AND q-1

e: NUMBER DISJOINT TO L

d: NUMBER SATISFYING (e x d) mod L = 1